EXHIBIT B-2

pointed out that OPM's "designated security officers" were appointed by, and report to, the program offices that own the systems, but "very few of the DSOs have any background in information security, and most are only managing their security responsibilities as a secondary duty to their primary job function."[147] The IG found that IT security at OPM was limited because "the OCIO has no authority to enforce security requirements" and concluded:

> IT security is a shared responsibility between the OCIO and program offices. The OCIO is responsible for overall information security governance while program offices are responsible for the security of the systems that they own. There is a balance that must be maintained between a consolidated and a distributed approach to managing IT security, but it is our opinion that OPM's approach is too decentralized. OPM program offices should continue to be responsible for maintaining security of the systems that they own, but the DSO responsibility for documenting, testing, and monitoring system security should be centralized within the OCIO.[148]

In other words, there were increasing calls for centralizing and fortifying authority and power under the OCIO by the OIG. By the end of FY2013, the centralized structure for information system security officers remained understaffed and hampered by budget restrictions.[149] And in 2013, as the agency prepared to transition to new leadership, the IG released two key reports. First, its newest FISMA audit found that the security of information systems remained a material weakness.[150]

Second, the IG also issued a warning about the information system where background investigation materials are stored. In June 2013, the IG audited OPM's Federal Investigative Services' Personnel Investigations Processing System (PIPS). The IG made clear the importance of this system:

> Approximately 15 million records of investigations conducted by and for OPM, the Federal Bureau of Investigations (FBI), the U.S. Department of State, the U.S. Secret Service, and other customer agencies are maintained in PIPS. Furthermore, the PIPS system interfaces with several other FIS systems to process applications while its data flow relies on both the OPM Local Area Network/ Wide Area Network (LAN/WAN) and Enterprise Server Infrastructure (ESI) general support systems.[151]

* * *

---

[147] *Id.*
[148] *Id.*
[149] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Federal Information Security Management Act Audit FY 2013*, at 5 (Nov. 21, 2013), https://www.opm.gov/our-inspector-general/reports/2013/federal-information-security-management-act-audit-fy-2013-4a-ci-00-13-021.pdf.
[150] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2013 to March 31, 2014*, at 10 (Mar. 2014), https://www.opm.gov/news/reports-publications/semi-annual-reports/sar50.pdf.
[151] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress April 1, 2013 to September 30, 2013*, at 7 (Sept. 2013) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar49.pdf.

> In the case of PIPS, we found that there were a number of controls inappropriately labeled in the system security plan as common or inherited. As a result, these **controls were never tested**, increasing the risk that these controls may not be functioning as intended, and therefore **posing a potential security threat to the system**. This omission is particularly concerning given the purpose of the system and the nature of the data the system contains.[152]

The IG's warning about the weakness in PIPS and the need to protect the background investigations data was prescient. The IG's warnings were in effect when, in 2013, the agency welcomed new senior leadership.

The Katherine Archuleta and Donna Seymour Era

On May 23, 2013, Katherine Archuleta was nominated to serve as Director of OPM.[153] The U.S. Senate confirmed Archuleta on October 30, 2013,[154] and she was sworn into office on November 4, 2013.[155] Archuleta was a former teacher, public administrator, community leader from Colorado and the National Political Director for President Obama's reelection campaign.[156] Shortly thereafter, in December 2013, Donna Seymour began her tenure as OPM's CIO.[157]

During her Senate confirmation hearing on July 16, 2013, Archuleta made a commitment to work with her senior management team to create a plan for modernizing IT within 100 days of assuming office, and to identify new IT leadership using existing agency expertise and with advice from government experts.[158]

As Archuleta and Seymour began their tenure, IT modernization was a key part of the Director's early agenda. Director Archuleta announced a new *Strategic Information Technology*

---

[152] *Id.*

[153] White House, Press Release, *President Obama Announces His Intent to Nominate Katherine Archuleta as Director of the Office of Personnel Management* (May 23, 2013), https://www.whitehouse.gov/the-press-office/2013/05/23/president-obama-announces-his-intent-nominate-katherine-archuleta-direct.

[154] Lisa Rein, "*Senate Confirms Katherine Archuleta as the Next Federal Personnel Chief*," WASH. POST, Oct. 30, 2013 available at: https://www.washingtonpost.com/politics/senate-confirms-katherine-archuleta-as-the-next-federal-personnel-chief/2013/10/30/65959bb0-41a6-11e3-a624-41d661b0bb78_story.html.

[155] U.S. Office of Pers. Mgmt., Press Release, *U.S. Office of Pers. Mgmt., Katherine Archuleta Sworn-In as 10th Director of the Office of Personnel Management: Greets Employees as the New Director and Gets to Work* (Nov. 4, 2013) available at: https://www.opm.gov/news/releases/2013/11/katherine-archuleta-sworn-in-as-10th-director-of-the-office-of-personnel-management/.

[156] Cecilia Muñoz, *Welcoming Katherine Archuleta, the First Latina Director of the Office of Personnel Management*, THE WHITE HOUSE (Nov. 4, 2013, 4:39 p.m.) available at: https://www.whitehouse.gov/blog/2013/11/04/welcoming-katherine-archuleta-first-latina-director-office-personnel-management.

[157] Jason Miller, *CIO Shuffle Continues at SBA, DHS, OPM*, FED. NEWS RADIO (Dec. 20, 2013), http://federalnewsradio.com/technology/2013/12/cio-shuffle-continues-at-sba-dhs-opm/.

[158] U.S. Office of Pers. Mgmt., *Strategic Information Technology Plan* (Feb. 2014) available at: https://www.opm.gov/about-us/budget-performance/strategic-plans/strategic-it-plan.pdf.

Plan in 85 working days (127 calendar days after being sworn in on November 4, 2013).[159] The Plan listed "Information Security" as one of six IT "Enabling Initiatives"—that is, initiatives to "provide the strong foundation necessary for successful operation, development, and management of IT that increases accountability, efficiency, and innovation."[160] The sixty-nine page report includes a brief discussion of the background investigation systems,[161] but the overall discussion related to background investigations focused largely on process reform and automation.[162] The Plan also included two-and-a-half pages on information security, wherein OPM stated it will:

- follow guidance from the *Federal Information Security Management Act*, NIST 800-53 ("Security and Privacy Controls for Federal Information Systems and Organizations");[163]
- follow guidance from OMB to ensure protection of these systems that contain PII and PHI [protected health information];
- work with DHS to implement continuous diagnostic monitoring (CDM) and use information security continuous monitoring (ISCM) tools;
- implement a three-phase plan to carry out its ISCM strategy; and
- attempt to secure additional resources to hire/train IT staff.[164]

Seymour later recounted early efforts to assemble the *Strategic Information Technology Plan* with Archuleta. In June 2014, Seymour testified to the Senate Committee on Homeland Security and Governmental Affairs:

> As Chief Information Officer (CIO) for the Office of Personnel Management (OPM), **I am responsible for the IT and innovative solutions that support OPM's mission** to recruit, retain, and honor a

[159] Joe Davidson, *OPM Unveils IT Plan to Improve Federal Retirement Operations, Recruitment*, WASH. POST, Mar. 10, 2014 available at: https://www.washingtonpost.com/politics/federal_government/opm-unveils-it-plan-to-improve-federal-retirement-operations-recruitment/2014/03/11/aee7db52-a92f-11e3-8599-ce7295b6851c_story.html.

[160] U.S. Office of Pers. Mgmt., *Strategic Information Technology Plan*, at vii (Feb. 2014).

[161] *Id.* at 32.

[162] The Plan's reference to background investigations included one line on security: "The initiative will also support reform in the investigative process and, drawing on the enabling initiative of information security, protect and secure the volume of sensitive information in the EPIC systems [the automated suite of background investigation systems]. U.S. Office of Pers. Mgmt., *Strategic Information Technology Plan* 32 (Feb. 2014).

[163] U.S. Dep't of Commerce, NIST Spec. Publ'n 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013) available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[164] U.S. Office of Pers. Mgmt., *Strategic Information Technology Plan* at 17-19 (Feb. 2014). Note: While OPM worked to craft the new Plan, key corresponding updates to key internal security guidance and protocols and Authority to Operation (ATOs). For example, OPM's "Incident and Response and Reporting Guide" was not updated—a guide issued in 2009. The Guide contains protocols for responding to breaches, among other things. *See* U.S. Office of Pers. Mgmt., *Incident Response and Reporting Guide* 3 (July 2009). *See also* Special Agent Tr. at 8. The OPM OIG special agent testified on October 6, 2015 that the *Incident Response and Reporting Guide* issued in 2009 was still the guidance in effect at OPM, as of October 2015.

world class workforce. Director Katherine Archuleta tasked me with conducting a thorough assessment of the state of IT at OPM – including how existing systems are managed and how new projects are developed. This process has led us to identify numerous opportunities for improvement in the way we manage IT….

Fulfilling the Director's promise, OPM released a Strategic IT Plan in March 2014. We developed the Strategic IT Plan to ensure our IT supports and aligns to our agency's Strategic Plan and that OPM's mission is fulfilled. It provides a framework for the use of data throughout the human resources lifecycle and establishes enabling successful practices and initiatives that define OPM's IT modernization efforts.

The plan also creates a flexible and sustainable Chief Information Officer (CIO) organization led by a strong senior executive with Federal experience in information technology, program management, and HR policy. OPM also understands that new IT implementation will be done in a way that leverages cybersecurity best practices and protects the personally identifiable information OPM is responsible for.[165]

Donna Seymour testifies to the Committee on Oversight and Government Reform

When Seymour testified before Congress in June 2014, however, **she did not mention that the agency learned in March 2014 of a significant data breach at the agency**; nor did

[165] *A More Efficient and Effective Government: Examining Federal IT Initiatives and the IT Workforce: Hearing Before the Subcomm. on Efficiency & Effectiveness of Fed. Programs & Fed. Workforce of the S. Comm. on Homeland Sec. & Gov't Affairs*, 113th Cong. (June 10, 2014) (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).

she mention that the agency, under her and Archuleta's watch, had spent the previous two months monitoring attackers and remediating a significant incident.[166]

On July 9, 2014, *The New York Times* broke the news, previously unknown to the public, that OPM suffered a breach.[167] *The Times* drew attention to the severe implications of the breach for anyone who had ever applied for a security clearance. The story stated:

> The intrusion at the Office of Personnel Management was particularly disturbing because it oversees a system called e-QIP, in which federal employees applying for security clearances enter their most personal information, including financial data. Federal employees who have had security clearances for some time are often required to update their personal information through the website. The agencies and the contractors use the information from e-QIP to investigate the employees and ultimately determine whether they should be granted security clearances, or have them updated.[168]

While *The Times* immediately grasped the potential implications for the country, OPM's CIO was trumpeting the merits of the agency's IT Modernization plan. In fact, OPM downplayed the damage from the breach to the *The Times*: The story stated:

> But in this case there was no announcement about the attack. 'The administration has never advocated that all intrusions be made public,' said Caitlin Hayden, a spokeswoman for the Obama administration. 'We have advocated that businesses that have suffered an intrusion notify customers if the intruder had access to consumers' personal information. We have also advocated that companies and agencies voluntarily share information about intrusions.'
>
> Ms. Hayden noted that the agency had intrusion-detection systems in place and notified other federal agencies, state and local governments about the attack, then shared relevant threat information with some in the security industry. Four months after the attack, Ms. Hayden said the Obama administration had no reason to believe personally identifiable information for employees was compromised.
>
> 'None of this differs from our normal response to similar threats,' Ms. Hayden said.[169]

---

[166] June 2014 OPM Incident Report; *see also, A More Efficient and Effective Government: Examining Federal IT Initiatives and the IT Workforce: Hearing Before the Subcomm. on Efficiency &Effectiveness of Fed. Programs & Fed. Workforce of the S. Comm. on Homeland Sec. & Gov't Affairs*, 113th Cong. (June 10, 2014) (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).

[167] Michael S. Schmidt, David E. Sanger & Nicole Perlroth, *Chinese Hackers Pursue Key Data on U.S. Workers*, N.Y. TIMES, July 9, 2014, available at: http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?_r=0.

[168] *Id.*

[169] *Id.*

Archuleta and Seymour later testified in 2015 that no PII was exfiltrated during the 2014 data breach.[170] Documents and testimony show gaps in OPM's audit logging practices led DHS to conclude the country will never know with complete certainty all of the documents the attackers exfiltrated during the breach discovered in March 2014.[171] It is clear, however, sensitive data was exfiltrated by the hackers.[172] As discussed in the following chapter, OPM watched the attackers steal documents related to OPM IT systems, including PIPs, contractor information, and documents containing names and the last four digits of associated Social Security numbers.[173]

Archuleta and Seymour did make some progress in addressing security governance issues by continuing to centralize IT security responsibility. They committed to make IT a priority with the release of their IT Modernization plan in early 2014, and arguably had more ownership of its IT security at this point than ever before. However, they failed to prioritize data security and implementation of basic cyber hygiene measures at a time when it became critically important to meet the increasing cyber threat.

Katherine Archuleta testifies to the Committee on Oversight and Government Reform

[170] *OPM Data Breach: Part II* (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.). During this hearing, then-Director of OPM, Katherine Archuleta, and then-CIO of OPM, Donna Seymour, testified nine times in a single exchange with Chairman Jason Chaffetz that no personally identifiable information was stolen.
[171] June 2014 OPM Incident Report at HOGR0818-001233-1246.
[172] The sensitivity of these documents is evidenced in part by the fact that OPM refused to produce these documents to the Committee in unredacted form until February 16, 2016. The Committee initially requested this information on August 18, 2015.
[173] June 2014 OPM Incident Report at HOGR0818 -001245-1246.

OPM Failed to Prioritize the Security of Key Data and Systems

OPM's failure to prioritize high-value targets like the background investigations data compounded the problems caused by inadequately investing in cybersecurity in the first place. Neither the data held by OPM, nor the access to OPM systems, were adequately protected. Indeed, OPM did not even have a complete IT inventory of servers, databases, and network devices.[174]

Further, on the system level OPM had not implemented multifactor authentication, making weak access controls a vulnerability that attackers were able to exploit.[175] OPM's failure to prioritize multifactor authentication implementation was a key observation that US-CERT made in their analysis of the data breach discovered in 2014.[176]

OPM was pressed about these and other issues during congressional hearings. For example, the background investigations data was not encrypted—encryption is the foundation of data-level security.[177] During a June 16, 2015 hearing before the Committee, Chairman Jason Chaffetz asked Director Archuleta why OPM did not use encryption, an industry best practice, and Director Archuleta said, "It is not feasible to implement on networks that are too old."[178]

Similarly, CIO Seymour told Ranking Member Elijah Cummings that the agency was working to use encryption. She testified:

> OPM has procured the tools, both for encryption of its databases, and we are in the process of applying those tools within our environment. But there are some of our legacy systems that may not be capable of accepting those types of encryption in the environment that they exist in today.[179]

In addition, key systems were also operating in FY 2014 without a valid Security Assessment and Authorization.[180] Also called "ATOs", authorizations to operate/authorities to operate provide a comprehensive assessment of the IT system's security controls. The OPM IG

---

[174] Office of Inspector General, U.S. Office of Pers. Mgmt., Report No. 4A-CI-00-15-011, *Federal Information Security Management Act Audit FY 2014* at i (Nov. 10, 2015) available at: https://www.opm.gov/our-inspector-general/reports/2015/federal-information-security-modernization-act-audit-fy-2015-final-audit-report-4a-ci-00-15-011.pdf

[175] *Information Technology Spending and Data Security at the Office of Personnel Management: Hearing Before the Subcomm. On Financial Serv.'s and Gen. Gov. of the Sen. Comm. on Appropriations,* 114th Cong. (June 23, 2015) (testimony of Richard Spires, former CIO of the Internal Revenue Serv.).

[176] *See Infra* Chapter 2.

[177] *Information Technology Spending and Data Security at the Office of Personnel Management: Hearing Before the Subcomm. On Financial Serv.'s and Gen. Gov. of the Sen. Comm. on Appropriations,* 114th Cong. (June 23, 2015) (testimony of Richard Spires, former CIO of the Internal Revenue Serv.).

[178] *OPM Data Breach, Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 16, 2015) (statement of Katherine Archuleta, Dir., U.S. Office of Pers. Mgmt.).

[179] *OPM Data Breach, Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 16, 2015) (statement of Katherine Archuleta, Dir., U.S. Office of Pers. Mgmt.).

[180] Office of the Inspector General, U.S. Office of Pers. Mgmt., *Federal Information Security Management Act Audit FY 2014* (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.

considers the authorization process to be a "critical step toward preventing security breaches and data loss."[181]

Of the 21 OPM systems due for reauthorization in FY 2014, 11 were not completed on time and were operating without a valid Authorization,[182] and several were among the most critical, containing the agency's most sensitive information.[183] This led the IG to warn OPM that "The drastic increase in the number of systems operating without a valid Authorization is alarming, and represents a systemic issue of inadequate planning by OPM program offices to authorize the information systems that they own."[184]

FISMA requires agencies to assess the effectiveness of their information security controls, the frequency of which is based on risk but no less than annually.[185] Appendix III of OMB Circular A-130, in place at the time, requires that agencies assess and authorize (formerly referred to as certify and accredit) their systems before placing them into operation and whenever there is a major change to the system, *but no less than every three years thereafter*.[186]

In November 2014, the IG's FISMA audit stated: "We therefore also recommend that OPM consider shutting down systems that do not have a current and valid Authorization."[187] OPM CIO Donna Seymour responded, however, that "The IT Program Managers will work with ISSOs to ensure that OPM systems maintain current ATOs and that there are no interruptions to OPM's mission and operations."[188]

Of the eleven major OPM information systems that were operating without a valid Authorization in FY2014,[189] three of these systems should have been an immediate priority for Director Archuleta and CIO Seymour to ensure were addressed: Personnel Investigations Processing System (PIPS), Enterprise Server Infrastructure (ESI), and the Local Area Network / Wide Area Network (LAN/WAN).

The security of these systems is critical because the flow of background investigation data through PIPs relies on both the OPM LAN/WAN and Enterprise Server Infrastructure (ESI) general support systems. LAN/WAN serves as the hardware and software infrastructure

---

[181] *Id.* at 11.
[182] *Id.* at 9.
[183] E-mail from Office of Pers. Mgmt. Inspector Gen. Staff to House Oversight & Gov't Reform Staff (Dec. 4, 2015) (on file with the Committee).
[184] U.S. Office of Personnel Mgmt. Office of the Inspector General, *Federal Information Security Management Act Audit FY 2014* at 9 (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.
[185] Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 44 U.S.C. § 3541 (2012).
[186] Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-130, Management of Federal Information Resources (Nov. 28, 2000) available at: https://www.whitehouse.gov/omb/circulars_a130_a130trans4/; see also U.S. Dep't of Homeland Sec., Security Authorization Process Guide 1 (Mar. 16, 2015) available at: https://www.dhs.gov/sites/default/files/publications/Security%20Authorization%20Process%20Guide_v11_1.pdf.
[187] Office of the Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CF-00-12-066, *Federal Information Security Management Act Audit FY 2014* at 2, 14 (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.
[188] *Id.*
[189] *Id.* at 9.

environment, supporting systems housed at OPM's Washington, D.C.; Macon, Georgia; and Boyers, PA facilities. LAN/WAN also supports the OPIS (PIPS imaging system)[190] and FTS (Fingerprint Transactional System). ESI is the general mainframe environment that supports PIPS. OPM's mainframe is considered a separate infrastructure or "general support system" from the LAN/WAN. PIPS, LAN/WAN and ESI were all operating on expired Authorities to Operate.[191]

The need to prioritize the security of these systems was well-known after the IG warned in June 2013 that PIPS had vulnerabilities, and that the "PIPS system interfaces with several other FIS systems to process applications while its data flow relies on both the OPM Local Area Network/ Wide Area Network (LAN/WAN) and Enterprise Server Infrastructure (ESI) general support systems."[192] However, the ATO for PIPS was not reauthorized in 2014, and the IG's FY2015 FISMA showed that "OPM's management of system Authorizations has deteriorated even further."[193]

Experts from outside OPM also criticized OPM's choices regarding IT security following the breach. On June 23, 2015, Richard Spires, the former CIO of the Internal Revenue Service and at DHS, testified before a Senate Committee on Appropriations' Subcommittee on Financial Services and General Government that OPM should have set better priorities and focused on securing the data itself rather than the systems as an initial priority. Spires stated:

> [I]f I had walked in there [OPM] as the CIO—and, you know, again, I'm speculating a bit, but—and I saw the kinds of lack of protections on very sensitive data, the first thing we would have been working on is how do we protect that data? OK? Not even talking about necessarily the

---

[190] OPIS was also operating with an invalid authorization to operate. *See* Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-IS-00-06-024, *Information Technology Security Controls of the Office of Personnel Management's Personnel Investigations Processing Imaging System* (July 11, 2006); *see also* E-mail from U.S. Office of Pers. Mgmt. Inspector Gen. Staff to House Oversight & Gov't Reform Staff (Dec. 4, 2015) (on file with the Committee).

[191] Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-IS-00-13-022, *Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Personnel Investigations Processing System FY2013* (June 24, 2013) available at: https://www.opm.gov/our-inspector-general/reports/2013/audit-of-the-information-technology-security-controls-of-the-us-office-of-personnel-managements-personnel-investigations-processing-system-fy-2013-4a-is-00-13-022.pdf; Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI-OO-ll-016, *Federal Information Security Management Act Audit FY 2012* (Nov. 5, 2012) available at: https://www.opm.gov/our-inspector-general/reports/2012/federal-information-security-management-act-audit-fy-2012.pdf; Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI-OO-12-014, *Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Local Area Network / Wide Area Network General Support System FY 2012* (May 16, 2012) available at: https://www.opm.gov/our-inspector-general/reports/2012/audit-of-the-information-technology-security-controls-of-the-office-of-personnel-managements-local-area-network-wide-area-network-general-support-system-fy-2012.pdf.

[192] Office of the Inspector General, U.S. Office of Pers. Mgmt., *Semiannual Report to Congress April 1, 2013 to September 30, 2013*, at 7 (Sept. 2013) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar49.pdf.

[193] Office of Inspector General, U.S. Office of Pers. Mgmt., Report No. 4A-CI-00-15-011, *Federal Information Security Management Act Audit FY 2014* (Nov. 10, 2015) available at: https://www.opm.gov/our-inspector-general/reports/2015/federal-information-security-modernization-act-audit-fy-2015-final-audit-report-4a-ci-00-15-011.pdf.

> systems. How is it we get better protections and then control access to that data better?[194]

Spires also stated that management issues posed a greater obstacle than resource problems in solving IT security problems. Spires testified:

> A focused effort on protecting the sensitive data with the right encryption and the right access-control capabilities, if you put the focus there, I think most federal agencies would have the funds, have the resources to be able to accomplish that.
>
> * * *
>
> Because of the sparse nature of the way IT has been run in a lot of agencies there are so many, let's say, inefficiencies that have crept into this system that I don't believe we effectively spend the IT dollars that we receive. So I believe that with the proper drive towards management you can actually derive a lot of savings from existing budgets.[195]

OPM has long been plagued by management's failure to prioritize information security in practice, and to retain leaders that are committed to information security over the long haul. Years of neglect, compounded by an abject failure of key leaders to make the right decisions at OPM in 2014, led to the worst data breach the federal government has ever experienced.

---

[194] *Information Technology Spending and Data Security at the Office of Personnel Management: Hearing Before the Subcomm. on Financial Serv.'s and General Gov. of the S. Comm. on Appropriations,* 114th Cong. (June 23, 2015) (testimony of Richard Spires, former Chief Info. Officer, Internal Revenue Serv.).

[195] *Id.*

Chapter 2: The First Alarm Bell – Attackers Discovered in 2014 Target Background Information Data and Exfiltrate System-Related Data

In the March 2014, US-CERT alerted OPM to an intrusion that laid the groundwork for the breach of OPM systems holding background investigation data, the "crown jewels" of current and former federal employees, contractors, and national security personnel.[196] OPM considered their response to the data breach, which they learned about from US-CERT in 2014, a success. CIO Donna Seymour touted the response strategy: "one of the things we were able to do immediately at OPM [in 2014] was recognize the problem. We were able to react to it by partnering with DHS . . . to put mitigations in place to better protect information."[197]

However, the data breach of background investigation data and personnel records first announced in June and July of 2015[198] raises serious questions about OPM's response to the data breach discovered in 2014. Documents and testimony obtained by the Committee show successes and failures, but some of the most important questions were unanswerable.

For example, while OPM testified that no personally identifiable information (PII) was exfiltrated during the 2014 data breach,[199] gaps in OPM's audit logging practices led DHS to conclude that the country will never know with complete certainty the universe of documents the attackers exfiltrated.[200] Documents and testimony show the materials exfiltrated from OPM likely would have given an adversary an advantage in hacking OPM's systems.[201] This evidence calls Donna Seymour's testimony into question. She told the Committee "**the adversaries in today's environment are typically [able] to use more modern technologies, and so in this case, potentially our antiquated technologies may have helped [OPM] a little bit.**"[202] In putting forward a "security through obscurity" defense, the CIO downplayed the reality that OPM was facing a determined and sophisticated actor while only having minimal visibility into their environment.

---

[196] June 2014 OPM Incident Report; *see also* David Perera & Joseph Marks, *Newly Disclosed Hack Got "Crown Jewels,"* POLITICO, June 12, 2015, available at: http://www.politico.com/story/2015/06/hackers-federal-employees-security-background-checks-118954.

[197] *Enhancing Cybersecurity of Third-Party Contractors and Vendors: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Apr. 22, 2015) (Question by Mr. Cummings).

[198] U.S. Office of Pers. Mgmt., Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015) available at: https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/; U.S. Office of Pers. Mgmt., Press Release, *OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats*, (July 9, 2015) available at: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.

[199] *Hearing on OPM Data Breach: Part II* (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.). During this hearing, then-Director of OPM, Katherine Archuleta, and then-CIO of OPM, Donna Seymour, testified nine times in a single exchange with Chairman Jason Chaffetz that no personally identifiable information was stolen.

[200] June 2014 OPM Incident Report *at* HOGR0818-001233 – 1246.

[201] Saulsbury Tr. at 27-28.

[202] *Enhancing Cybersecurity of Third-Party Contractors and Vendors: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (2015) (Question by Mr. Cummings).

In the aftermath of their 2014 response, available threat intelligence about the relevant actor groups targeting federal employee information and the types of malware discovered in 2014 also raised the stakes for OPM. In the fall of 2014, Novetta and a number of supporting industry organizations produced a detailed report containing information pertinent to Chinese APT activity with an emphasis on Hikit malware. This malware was found during the 2014 incident response. The Novetta paper specifically looked at the Axiom Threat Actor Group, which according to public reports, was responsible for the OPM data breach discovered in 2014.[203] The analysis warned that among the industries being targeted or infected by Hikit were Western government agencies with responsibility for personnel management. The report also warned that "[w]ithin these targets, Axiom has been observed as going out of its way to ensure continued access regardless of changes to its target's network topology or security controls."[204]

OPM leadership downplayed the significance of the 2014 breach. Instead, OPM should have raised the alarm and recognized this initial attack as a serious and potentially devastating precursor given how close the early attackers got to the background investigation systems and the related data taken during this breach. The following discussion describes OPM's 2014 discovery and incident response efforts, and how Hikit malware was found and sensitive data related to the background investigation function was taken from OPM's systems. Further, this discussion highlights key observations that were made about the weaknesses and vulnerabilities of OPM's IT security during this incident response period.

Discovery & Incident Response for Attackers Discovered in 2014

On March 20, 2014, OPM's Computer Incident Response Team (CIRT) received notification from DHS' US-CERT that data had been exfiltrated from OPM's network.[205] Beginning March 2014 and through May 2014, OPM (in consultation with US-CERT) investigated the incident, monitored the attacker, developed and implemented a mitigation plan, and removed this initial attacker from OPM's system.

US-CERT notified OPM that a third party had reported data being exfiltrated from OPM's system to a known command and control server (C2).[206] Jeffrey Wagner, OPM's Director of IT Security, testified about OPM activities upon notice from US-CERT:

> [T]he initial response [to the 2014 data breach] is a 3/20 call from DHS. All right. So on 3/20 DHS called us and let us know, hey, we think this is bad. We began pulling logs, and records, and things of that nature, and on 3/25 is when we verified that it was a malicious activity.[207]

---

[203] Novetta Operation SMN: Axiom Threat Actor Group Report.
[204] *Id.* 8-9.
[205] June 2014 OPM Incident Report at HOGR0818-001233.
[206] *Id.* OPM contractor Brendan Saulsbury stated that "[the 2014 incident] was first detected by US-CERT via the Einstein appliances that they have on [OPM's] network. And that was communicated to OPM via email." Saulsbury Tr. at 13. The OPM Incident Report states that a "third party" reported the data exfiltration to DHS. June 2014 OPM Incident Report at HOGR0818 -001233. It is possible that both accounts are correct and that the "third party" referenced in the 2014 Incident Report is an Internet Service Provider who reported network activity collected by an Einstein sensor.
[207] Wagner Tr. at 13.

Wagner also described OPM's process for analyzing and elevating information security reporting or alerts to a cybersecurity incident. He stated:

> Once we get forensic evidence that there's actual adversary activity within the environment, it escalates the level of response. So, for instance, on a regular basis we get alerts or reports of an email trying to be sent to us that has a malicious link. It creates an alert. We'll do initial forensics on that alert, and we'll see that our current tools will stop that malicious link from being able to connect or downloading anything. And it de-escalates the situation. So from an incident response perspective, everything rises to a critical level, and then once we have forensics evidence and identify specifically what is going on, and it then escalates into the specific response required.[208]

As OPM's incident response activities began, documents show that as of March 20, 2014, the following facts were among those known to OPM:

- FIS Investigator accounts had been compromised.
- The malicious C2 server was communicating with an OPM server.
- The malicious C2 servers' communications with OPM were encrypted.[209]

During the incident response period, OPM learned the C2 server was connecting with an OPM network monitoring server ([redacted]) between the hours of 10 p.m. and 10 a.m.; then the attackers were using this server and a compromised Windows domain administrator credential to search for PIPs-related files on OPM's network.[210] An initial examination of the network traffic between the [redacted] server and the C2 server found that the communications were encrypted utilizing a four byte XOR key, indicating a specific intent to disguise themselves amongst network traffic.[211]

Brendan Saulsbury, an OPM contractor working in the OPM IT Security Operation group, testified that OPM used the security tool NetWitness to identify what devices on OPM's network were actively communicating, or "beaconing" to the C2 server.[212] Using the network traffic information gathered by NetWitness, Saulsbury was able to design a custom script to "reverse engineer the obfuscation algorithm the attackers were using to mask their traffic so it would not be detected by sensors, like [OPM's] security tools."[213] Saulsbury's team could then

---

[208] *Id.*
[209] June 2014 OPM Incident Report at HOGR0818 -001240.
[210] *Id.* at HOGR0818-001233.
[211] *Id.* An XOR key encryption, or exclusive-or encryption is a form of private key encryption that relies upon a simple binary formula to develop its obfuscation of the underlying data.
[212] Saulsbury Tr. at 39.
[213] Saulsbury Tr. at 40.

observe the infected machines communicating with the C2 server, and also the commands that were being sent down from the "actual attacker sitting at the keyboard."[214]

Thus, OPM and their interagency team were able to identify the adversary's initial foothold in OPM's network—where the attackers had established a persistent presence in the environment. Once it was determined which devices on OPM's network were beaconing to the hackers' C2 server, OPM was in a position to begin a full forensic investigation and look for malware on the compromised machines.[215] On or about March 25, in the words of OPM Director of Security Operations Jeff Wagner, a "critical level"[216] was reached and OPM was able to make a "full determination on the who and what"[217] of the data breach, to know where the hackers are "going, what they are seeing," and most importantly "what [the hackers] are interested in."[218] As a result, OPM determined the incident was malicious on March 25, 2014, moved DHS onsite to assist the response, and began a full monitoring phase to gather information to answer the question of "how."[219]

During the three-month incident response period, OPM undertook a number of other incident response activities. For example, according to US-CERT's 2014 Report timeline, on March 26, 2014 OPM searched for embedded malware on end points at its Washington, D.C. headquarters, at its Boyers, Pennsylvania data center, and at a back-up data center in Macon, Georgia.[220] On March 27, 2014, OPM took steps to remediate the OPM Personnel Investigations Processing System Imaging System (OPIS)—a system that provides an electronic representation of case paper files to expedite the processing of background investigations – and performed this remediation work in late March.[221] On March 28, 2014, in recognition of the fact that OPM did not have the ability to monitor traffic in and out of PIPS – the system that held background investigation data – OPM installed a fiber tap to begin to monitor such traffic. Finally, during this period OPM watched the attackers take sensitive data relating to high-valued targets on OPM's systems, such as the PIPS system.[222] OPM was never able to determine how the adversary initially entered their systems.

Then from late March through April 2014 the incident response team continued to identify additional infected workstations and malware on key systems.[223] Specifically, OPM found Hikit malware on several OPM systems.[224] Hikit is a variant of rootkit malware (which is "an extremely stealthy form of malware designed to hide its malicious processes and programs from the detection of commodity intrusion detection and anti-virus products").[225] As US-CERT

---

[214] Saulsbury Tr. at 40.
[215] Saulsbury Tr. at 39-40.
[216] Wagner Tr. at 13.
[217] June 2014 OPM Incident Report at HOGR0818 -001240.
[218] *Id.*
[219] *Id.*
[220] June 2014 OPM Incident Report at HOGR0818 -001241.
[221] *Id.*; *see also* Office of Pers. Mgmt., *OPM Personnel Investigations Processing System Imaging System (OPIS) Privacy Impact Assessment* available at: https://www.opm.gov/information-management/privacy-policy/privacy-policy/pips-imagingsystem.pdf.
[222] June 2014 OPM Incident Report at HOGR0818-001234.
[223] June 2014 OPM Incident Report at HOGR0818-001241-1242.
[224] June 2014 OPM Incident Report at HOGR0818-001234; *Id.* at Appendix C.
[225] June 2014 OPM Incident Report at HOGR0818-001234.

explained in the June 2014 OPM Incident Report, "HiKit allows the attacker to run commands and perform functions from a remote location as if they had the equivalent of a monitor and keyboard connected to the compromised OPM system."[226]

Time is crucial in an incident response scenario. According to NIST, "organizations should strive to detect and validate malware incidents rapidly because infections can spread through an organization within a matter of minutes."[227] The agency's slow response made matters worse. According to NIST, "minimizing the number of infected systems, which will lessen the magnitude of the recovery effort."[228]

Once the incident was identified and OPM, along with their interagency partners, entered into an advanced monitoring phase necessary intelligence was gathered on the adversaries' tactics, techniques, and procedures, the kind of threat information necessary to harden information security not only at OPM but at other agencies.

Monitoring the Adversary and the May 2014 "Big Bang" to Expel Attackers Discovered in 2014

From March 25, 2014 to May 27, 2014, OPM, upon the advice of US-CERT, engaged in a prolonged intelligence gathering phase. The goal of this advanced monitoring phase was to "carefully observe all of the malicious actors' activities in order to gain an understanding of their tactics, techniques, and procedures (TTPs) as well as to identify all of their other unknown or inactive infected systems within OPM's network."[229] The advanced monitoring of the adversary ended in a "Big Bang" on May 27, 2014—an effort that commenced once the hackers got "too close" to the background investigation material accessible from the PIPS system.[230]

Saulsbury described the comprehensive monitoring strategy during a transcribed interview with Committee investigators. He testified:

> [US-CERT's] advice was to basically do an ongoing investigation and figure out, do our best to find the entire attacker foothold in the network and then remediate them all at once to prevent the attacker from realizing that you are aware of them, and then changing their tactics and techniques to further avoid detection.[231]

Wagner also described the scope of the monitoring phase. He testified that OPM was not just looking for TTPS, but other indicators. Wagner stated:

---

[226] June 2014 OPM Incident Report at HOGR0818-001234.
[227] Peter Mell, Karen Kent & Joseph Nusbaum, Nat'l Inst. of Standards & Tech., Spec. Publication 800-83, *Guide to Malware Incident Prevention and Handling* 3 (Nov. 2005) available at: http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.
[228] *Id.*
[229] June 2014 OPM Incident Report at HOGR0818 -001233.
[230] Saulsbury Tr. at 26.
[231] Saulsbury Tr. at 25-26.

> You're trying to find specific actions they're doing to give you an indication of what they're doing and what they want. You're also looking for -- as a former pen tester, usually what you try to do to try to prevent people from catching you, is you try to set up other back doors or means in which you can create a persistent attack. It's just making sure you always have a secondary way in.[232]

In US-CERT's June 2014 OPM Incident Report, there is almost a daily catalogue of OPM's monitoring efforts. As part of the monitoring effort, OPM established a series of alerts and system rules to watch the adversary, employing a full packet capture (logging data) tool to gather network traffic between the infected machines and the C2 server.[233] An interagency team, including DHS, FBI, and NSA,[234] was involved in the incident response effort. The team received automatic notifications during the monitoring phase.[235] During this 2014 incident response period, OPM used its existing set of security tools and infrastructure to conduct their monitoring effort.[236]

In addition to monitoring, OPM was prepared to implement preventative measures. For example, Wagner testified that they were instructed to shutoff internet access if any PII was leaving the network.[237] By March 27, 2014, US-CERT reported that OPM had "heightened proactive readiness" and was developing plans for "full shutdown."[238] By April 11, 2014, tactical mitigation strategy and security remediation plans were being developed to eliminate the adversary's foothold on OPM's network.[239] The process of setting up alerts and tipping points, identifying infected workstations, and elevating monitoring technology continued until the "Big Bang" on May 27, 2014.

While the US-CERT timeline is helpful to understand the 2014 incident response activities, some entries illustrate gaps in OPM's visibility into their systems and applications, including the highly sensitive PIPs system – which housed the sensitive background investigation data. For example, the March 28, 2014 timeline entry states OPM "did not have [the] ability to monitor traffic in/out of PIPS – Installed PIPS fiber tap."[240] Wagner responded to this entry by testifying:

> So in that specific instance -- a mainframe functions significantly different

---

[232] Wagner Tr. at 15.
[233] June 2014 OPM Incident Report at HOGR0818 -001240.
[234] Saulsbury Tr. at 43 ("US-CERT brought the NSA Blue Team onsite.").
[235] Wagner Tr. at 59 ("So if the adversary's activity was from 10 p.m. to 10 a.m. but it was normally in a period of 3 to 4 a.m. where they were active, when they would throw something on our network or send a script to the network, I would get a phone call. I would then call DHS and FBI. So it was a concerted effort. It wasn't simply OPM by itself.").
[236] June 2014 OPM Incident Report at HOGR0818 -001233.
[237] Wagner Tr. at 10 (The question posed to Mr. Wagner was whether or not the security staff at OPM had the authority to make operational decisions; his answer stated that "I guess a good example would be during the 2014 or 2015 breaches, the security operations group was under a standing order from the director that if we indicated that information was leaving, we could shut down the Internet at any time.").
[238] June 2014 OPM Incident Report at HOGR0818 -001241.
[239] *Id.*
[240] *Id.*

> from a standard distributing environment, say Linux, or Windows, or like you have at your home. A mainframe is a giant cloud computer, which runs on a proprietary type operating system, and it communicates in a far different method than a standard distributing environment. So at the time we did not have equipment installed to try to navigate between distributed and mainframe. We had a project to implement these pieces, and what we did is we sped up the project to get the fiber taps installed to be able to set up a communication method to where we could see the traffic as it traversed between the distributing environment and the mainframe environment.[241]

Saulsbury also described OPM's limited ability to monitor Internet traffic during and prior to the 2014 incident. He testified:

> OPM had the ability to monitor traffic going out to the Internet at all times or at least going back prior to the 2014 incident. The reason for putting a network tap on the PIPS segment is to be able to monitor what is called, what we refer to as east-west traffic, so internal-to-internal traffic, from the general network going in and out of PIPS.[242]

It was not until March 31, 2014 that OPM was able to "turn on" the monitoring capabilities for all PIPS and Federal Investigative Services (FIS) related systems.[243] In other words, it took almost eleven days from the time OPM was notified on March 20, 2014 about the data breach for OPM to deploy the capabilities necessary to monitor one of the most high value targets on their IT environment – PIPs.

The US-CERT timeline also highlights other gaps in OPM's information security posture that made OPM vulnerable to attack and put sensitive data OPM held at risk. For example, a March 31, 2014 entry states: "high value, targeted users only needed to authenticate with username and password, which could be compromised remotely – Enforced PIV access for 5 high-value users."[244] Jeff Wagner testified about challenges related to implementing PIV functionality:

> Q. Were they not being enforced prior to that?
>
> A. No.
>
> Q. Why was that?
>
> A. It was a project that was on the list, and to completely change the culture and the functionality of some systems, it takes planning.

[241] Wagner Tr. at 19-20.
[242] Saulsbury Tr. at 35.
[243] June 2014 OPM Incident Report at HOGR0818 -001241.
[244] June 2014 OPM Incident Report at HOGR0818 -001242.

Q. When you say the culture of some systems, what do you mean by that?

A. So as users have built systems throughout years or decades, they have become accustomed, and there's business or operational procedures that rely on specific methods. In order to change authentication methods from like user name password to PIV, some of those processes have to get redefined and republished.[245]

Thus, the challenge of fully enforcing multifactor authentication through the use of PIV cards arose in part from the agency's culture. Wagner testified that maintaining the functionality of the production environment was related challenge in deploying PIV. He said: "full deployment of PIV, caused certain applications and certain functionalities to break."[246] Wagner testified that in response to the 2014 breach remediation plan, 100 percent of windows administrators began utilizing PIV cards through an Xceedium appliance,[247] and by September 2014, all OPM users were PIV compliant.[248] According to an OMB Report on Fiscal Year 2014 activities, OPM still had not fully implemented PIV card access rules. OPM was identified in this OMB Report as one of several agencies with the "weakest authentication profile[s]" – meaning a majority of the agency's unprivileged users logged on only with a user ID and password, making an unauthorized access more likely.[249]

While OPM monitored the situation in 2014 to the extent their 2014 security posture allowed, the next step was to develop a remediation plan to eliminate the attackers' presence on the OPM's network. Prior to the May 27, 2014 "Big Bang" effort to eliminate the attackers from OPM's network, OPM began taking other ad hoc measures to mitigate the damage. In early May, OPM began setting up "green zones" —the security team's effort to "eliminate certain administrators from being on the network to be exploited."[250] Wagner described the green zone during his testimony. He stated the green zone was:

---

[245] Wagner Tr. at 38.
[246] *Id.*
[247] Wagner Tr. at 74 (Mr. Wagner testified that, "There is a piece of network equipment that needs to get purchased and installed to finalize the last couple pieces at the Macon site. But to clarify, they're all forced to utilize PIV through the Xceedium Appliance. There just happens to be a potential workaround that we have mitigation pieces in place to prevent.").
[248] Wagner Tr. at 75 (explaining that the exact date that all administrator accounts began PIV compliant varied based upon the location). As of April 2015, OPM reported to OMB that 100 percent of their privileged users were required to use PIV cards and only 41 percent of their unprivileged users were required to use PIV cards. After a 30 day cyber sprint launched in July 2015, OPM reported 97 percent PIV card compliance as of July 2015. Office of Mgmt. & Budget, Exec. Office of the President, *CyberSprint Results* (July 31, 2015) (On file with the Committee).
[249] Office of Mgmt. & Budget, Exec. Office of the President, *Annual Report to Congress: Federal Information Security Management Act* 23 (Feb. 27, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf. PIV cards facilitate multifactor authentication credentials to control access. Such technology can at a minimum slow attackers who attempt to use unsecure credentials to move around an IT network. Memorandum from Jacob J. Lew, Dir., Office of Mgmt. & Budget, Exec. Office of the President, to Heads of Exec. Dep'ts. and Agencies, M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors* (Feb. 3, 2011), https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf. .
[250] Wagner Tr. at 137-138.

> [A] creation of independent machines that the database administrators utilizing that was wholly separate from the normal network so that all database access of the database that we knew [the adversaries] were looking for could only be accessed through this one controlled machine, which was not on the network.[251]

Green zone machines were configured at locations in Washington, D.C. and Boyers, Pennsylvania. Deployment and configuration of the green zone workstations continued through May 23, 2014.

Between May 23 and May 27, the US-CERT timeline does not provide a clear description of activities prior to the May 27, 2014 "Big Bang" effort to eliminate the attackers nor provide the reason after two months of monitor May 27 was the designated date.[252] However, testimony given before the Committee does fill in some of this gap. Wagner testified:

> We needed preparation to do the Big Bang. The three-day weekend was coming up. It was something that looked like a perfect time to prestage everything. However, we wanted to ensure that the users were involved and we could get full direct identity of the users when changing passwords. We didn't want to just get a phone call from somebody saying, hey, I need my password changed. We wanted to be able to physically verify that passwords were being changed by users. So that date was specifically chose to prestage all the back-end processes that needed to be in place in order for a full-user reset.[253]

Wagner stated the decision to remove the adversary from the agency's network on May 27 was made as a result of the forensic analysis process and not necessarily related to how close the adversary got to the background investigation system (PIPs). He testified:

> Q. So beyond the period of time to stage the event, were the attackers moving in the network they gave you an indication that you needed to kick them out at this point? Were they getting close to PII? Were they getting close to –
>
> A. It was a point of presence in which the interagency response team felt that there was nothing more to be gleaned from the presence of the adversary. We weren't learning anything new. They weren't searching for anything different. And so the risk of kicking them out too early had come and gone, and now the risk was becoming having them in too long, and we didn't want to keep them around any longer than we had to.[254]

---

[251] Wagner Tr. at 137-138.
[252] June 2014 OPM Incident Report at HOGR0818 -001243.
[253] Wagner Tr. at 39.
[254] Wagner Tr. at 39-40.

Wagner's testimony—that OPM and their interagency partners were no longer gaining useful intelligence from the monitoring phase—is at odds with the testimony of Brendan Saulsbury, an OPM contractor with OPM's IT Security Operations who played a significant role in monitoring the attackers during this period. Saulsbury stated:

> Q. And you and your team were monitoring their penetration. And was there any particular danger that precipitated the decision to conduct the Big Bang when it was conducted?
>
> A. Yes. So we would sort of observe the attacker every day or, you know, every couple of days get on the network and perform various commands. And so we could sort of see what they were looking for. They might take some documentation, come back, and then access, you know, somebody else's file share that might be a little bit closer or have more access into the system. We would sort of see them progress as we are doing our investigation. **And then it got to the point where we observed them load a key logger onto a database administrator's work station, or actually several database administrators' workstations. At that point, the decision was made that they are too close and OPM needs to remove whatever they were aware of at the time.**
>
> Q. Okay. And that precipitated the Big Bang. When you say too close?
>
> A. **They were too close to getting access to the PIPs system.**[255]

The distinction is significant on two levels. First, if Mr. Saulsbury is correct, it is possible that OPM had not yet identified all of the infected systems on their network, i.e. the agency had not yet identified the scope of the hacker's foothold. Second, if the adversary was getting "too close" to the PIPS system it is likely the hacker had conducted sufficient reconnaissance of OPM's network to access that application, but had not yet successfully executed the end-stage of their hack and successfully exfiltrated data.

Regardless of the instigating events, the first phase of the remediation plan (the "Big Bang") was completed on May 27, 2014.[256] OPM took a number of steps in collaboration with US-CERT to "eradicate the malicious actor, at least temporarily, from OPM's network." These steps included: removing all known compromised systems, creating new accounts for 150 known or potentially compromised users and disabling their old accounts, and forcing all Windows administrators to use PIV card for authentication.[257]

---

[255] Saulsbury Tr. at 25-26.
[256] Saulsbury Tr. at 48; Wagner Tr. at 57 (Wagner referring to the end of the monitoring phase as the "Big Bang").
[257] June 2014 OPM Incident Report at HOGR0818-001235.

In addition, the "Big Bang" effort included: resetting administrative accounts; PIV-enforcing all admin accounts; building new accounts for compromised users; resetting all local accounts on all servers; taking the compromised systems off line; and a "stateful" reset of all internet routers.[258] OPM and their interagency partners were effectively attempting to press the reset button and eliminate the adversary's foothold in OPM's environment by eliminating their means of mobility (user accounts) and presence (compromised systems).

OPM continued remediation efforts and was confident the adversary had been removed from their environment. Jeff Wagner, OPM's Director of IT Security Operations testified:

> DHS remained with their Mandiant tool for another 30 or 45 days. We even had regular checkups with US-CERT, where I'd go over to the [redacted] and talk to them to see if there was any communication throughout DHS, FBI, the IC community, if anything that was being identified related to OPM, and there was no communication whatsoever.[259]

Documents and testimony show OPM leveraged both interagency partners and private sector technologies, including Mandiant,[260] to ensure their systems, particularly the PIPS system, were clean of any malicious presence. Saulsbury testified: "The NSA blue team came into OPM and they were performing both vulnerability scans, and scans for malware artifacts on the network."[261]

Wagner and Saulsbury admitted, however, that the attack OPM discovered in 2015 – which led to the exfiltration of background investigation data in the summer of 2014 – was already underway during the 2014 incident response period and continued after the Big Bang.[262] On or about May 7, 2014 and while OPM was closely monitoring the OPM network, the attackers had established a foothold and dropped malware.[263]

[258] June 2014 OPM Incident Report at HOGR0818 -001243.
[259] Wagner Tr. at 40.
[260] Wagner at 54 ("They also deployed some of their technical staff to deploy the Mandiant tool. We didn't have at the time a deployed endpoint search mechanism. So they deployed their Mandiant to our environment to do the search for malware. Actually, there's another component. They also utilized their forensics team to do some of the forensic imaging and then malware analysis once they took the drives -- occasionally took the drives back to DHS headquarters -- DHS office on Glebe to do analysis, forensics analysis.").
[261] Saulsbury Tr. at 27.
[262] Wagner Tr. at 127-128; Saulsbury Tr. at 70-71.
[263] *Id.*

During the 2014 Incident Response Period the Exfiltration of PIPS-related Information Made Clear the Attackers' Target was Background Investigation Data Held in PIPS

During the 2014 incident response period while OPM was monitoring the attackers, OPM observed the exfiltration of data related to the PIPs system. The fact that this information was taken makes clear the target; further, this information likely informed the background investigation data exfiltration that was later discovered in 2015. US-CERT's June 2014 Incident Report Appendix D lists the data exfiltrated while OPM monitored their network in 2014.

Appendix D - Exfiltrated OPM Data

Document Name	Contains PII?
PIPS SAR with CA package April 2008.pdf	No
PIPS.PDF	No
PIPS_PFIS_GFIS Business Processing.DOC	No
EPIC Briefing for CIO v5.ppt	No
EPIC-eQIP only.vsd	No
OPM IAS Modernization Alternatives and Recommendation_v15 81607.doc	No
OPM IAS Business Case_Appendices_v15 81607 - APPENDIX M ONLY2.doc	No
Visio-Phase 1 - Application Creation.pdf	No
Visio-Phase 2 - Application Processing.pdf	No
Visio-Phase 3 - Investigation.pdf	No
Visio-Phase 4 - Case Closing.pdf	No
PIPS IT-Web submission - 9-10-07.pdf.zip	No
PIPS IP Systems & Services on zSeries v3.pdf	No
ZOS Con to Network 02012008.vsd	No
PIPS Data for UPN Match.xlsx	No (Names, Last 4 SSN)
PIPS Fed-Employee List for IT Awareness-2014.txt	No (Names, Last 4 SSN)
PIPS Outside-Agy List for IT Awareness-2014.txt	No (Names, Last 4 SSN)
PIPS Disaster Recovery url	No
PIPS Programmer Groups.docx	No
pips contractor list 2009.xls	No
PIPS Pgmr Group Access.txt	No
PIPS Pgmr in AP group list.txt	No
PIPS_User Matrix-2-7-2010.xls	No
PIPS-For-UPN.zip	Password Protected (Unable to Open)
PIPS Contractor List for IT Awareness-2014.txt	No (Names, Last 4 SSN, Company)
PIPS EPIC Iteration 1 Dictionary.xls	No
PIPS_Print_Solution_PageCenter.ppt	No
PIPS Batch Job Frequency.xls	No
PIPS-2B-Mapping.xlsx	No
PIPS-R Deletes.xlsx	No
PIPS-R File Usage Data 20090323.xls	No
PIPS_Cluster_Conversion_Plan.xls	No

By way of background, OPM's PIPS is a mainframe application on the OPM environment that stores the background investigation information provided by employees and perspective employees on forms SF-86, SF-85, and SF85P.[264] PIPS interacts with several other

[264] Wagner Tr. at 19; U.S. Office of Pers. Mgmt., *Federal Investigative Service Division Information Technology Privacy Impact Assessment* 43 (Oct. 2006).

Federal Investigative Services (FIS) systems and the connected and component databases contain information and materials that are considered the "crown jewels" for a foreign intelligence service.[265]

Based on the nature of the information held in the PIPS and related systems it was clearly a target, but Jeff Wagner OPM's Director of IT Security Operations seemed to downplay the significant of PIPS as a target. He testified:

> Q. What is the PIP server or system?
>
> A. PIPS is an application that sits on the mainframe.
>
> Q. Why would that be a target for an adversary, that particular application?
>
> A. It's a large data repository.
>
> Q. It's a high-value target?
>
> A. It's currently assessed as a high-value assessment, but it's a large data repository. Any large data repository is always a target.[266]

The PIPs system is more than simply a "large data repository." The data it stores—sensitive background investigation information gathered from SF-86 forms—is some of the government's most valuable PII.[267] Documents that could inform attackers about the nature of and the architecture of PIPS and related systems should not have been permitted to be exfiltrated from OPM's network.

Appendix D (as shown above) lists documents that were exfiltrated during OPM's monitoring effort in 2014. The documents relate to OPM IT systems, including PIPs, contractor information, and documents with names and the last four digits of those individuals' Social Security numbers.[268] Additionally, the documents listed in Appendix D contain information relevant to large repositories of PII information. The list of "Exfiltrated OPM Data" in Appendix D identifies 34 documents.[269] Appendix D indicates none of the documents contained PII (except in one case where the PII was password protected and the adversary was unable to open

---

[265] David Perera & Joseph Marks, *Newly Disclosed Hack Got "Crown Jewels,"* POLITICO, June 12, 2015, available at: http://www.politico.com/story/2015/06/hackers-federal-employees-security-background-checks-118954.

[266] Wagner Tr. at 19.

[267] According to NIST guidance, "PII is —any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." *See* National Institute for Standards and Technology, Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

[268] June 2014 OPM Incident Report Appendix D at HOGR0818 -001245-1246.

[269] *Id.*

it). Four of the documents, however, included the last four digits of individual Social Security numbers.[270]

In describing the items exfiltrated in Appendix D, US-CERT's June 2014 Incident Report makes clear the target was PIPS. The Report stated:

> The attackers primarily focused on utilizing SMB [Server Message Block] commands to **map network file shares of OPM users who had administrator access or were knowledgeable of OPM's PIPs system**. The attackers would create a shopping list of the available documents contained on the network file shares. After reviewing the shopping list of available documents, the attackers would return to copy, compress, and exfiltrate the documents of interest from a compromised OPM system to a C2 server.[271]

Further, there remains the important caveat from US-CERT that additional documents may have been exfiltrated prior to OPM's monitoring phase which began in March 2014. US-CERT stated:

> In should be noted the attackers had **access to OPM's network since July 2012** and the documents [] were exfiltrated during the time period of March 2014 to May 2014 when OPM [] stated their advanced monitoring of the infected systems. **Additional documents may have been exfiltrated prior to March 2014, but there is no way to determine with exact certainty**.[272]

Wagner downplayed the significance of the information exfiltrated in 2014 and testified that the information was "standard" and would not necessarily give an adversary an advantage in a subsequent attack.[273] He testified:

> A. So all of -- so in 2014, the adversary was utilizing a visual basic script to scan all of our unstructured data. So the data comes in two forms. It's either structured, i.e., a database, or unstructured, like file shares or the home drive of your computer, things of that nature. All the data that is listed here, all came out of personal file shares that were stored in the domain storage network. And when I went back to the program offices and had them sit down with us and do an assessment of it and look at the age and the amount of data within these, it was not recognized to be critical data or critical information. It's pretty standard documentation, for the most part.

---

[270] *Id.*
[271] June 2014 OPM Incident Report at HOGR0818 -001234-1235.
[272] June 2014 OPM Incident Report at HOGR0818 -001235.
[273] Notably, OPM produced these documents from Appendix D to the Committee in the Fall of 2015 with redactions and in camera. It was only under subpoena that OPM produced these documents without redactions in February 2016.

Q. When you say "standard documentation," documentation that would be public accessible?

A. I don't necessarily know if it would totally be publicly accessible. I don't know what everyone publishes. But like A&A and C&A packages, for the most part, are available for review; they're traded amongst agencies. It's not something you would be, you know, overly freaked out over.[274]

When questioned further about the significance of the Appendix D documents, Wagner continued to downplay the significance of these documents in his testimony:

Q. One of the entries includes a document that was exfiltrated PIPS contractor list [redacted] Is that the kind of information that you would want in the hands -- not that you would want in the hands of an attacker -- but that would give an attacker an advantage?

A. The list of contractors from 2009 was just simply a user name list of the system. It's not something that's -- it wouldn't necessarily give them an advantage. I mean –

Q. Would knowing the users on a network for a particular system –

A. Finding users is not difficult. For the most part, if you think about it, most companies or agencies utilize a standard-type naming scheme. So it's fairly easy from a pen tester or an adversary standpoint to glean this information, either from initial presence or half the time you can just Google it. For instance, everybody's Facebook account utilizes a Yahoo or a Google email address. It wouldn't be difficult to find anyone, any individual's credentials in some form to figure out what your user name to your Facebook is.[275]

Saulsbury, however, disagreed with Wagner's assessment of the sensitivity of the Appendix D documents that were exfiltrated. He testified that the documents could be useful to the hackers in a subsequent attack. He stated:

Q. So tell me first of all, are these public things that OPM would be concerned about if they were put out into the open?

A. Yes, these are not documents that are meant to be public.

Q. And what kind of documents are these if you could generally characterize them?

[274] Wagner Tr. at 41.
[275] Wagner Tr. at 42.

A. They are basically, sort of system documentation, various processes, and related to the background investigation systems.

Q. So if an attacker were able to exfiltrate this type of data, which it appears they did, would this give them an advantage for a future attack?

A. Yes.

Q. And how so?

A. **It gives them more familiarity with how the systems are architected. Potentially some of these documents may contain accounts, account names, or machine names, or IP addresses, that are relevant to these critical systems.**[276]

Saulsbury's testimony indicates the exfiltrated documents in Appendix D contained information relevant to understanding "how the system works." These documents included among other things a 2014 list of contractors with access to the PIPS system, a CIO-level briefing on the EPIC system and a discussion of the interface between the PIPS and Joint Personnel Adjudication System (JPAS) systems. These documents would have improved an adversary's understanding of OPM's system, its architecture, and information on who has access to the background investigation information contained on the PIPS system. The Appendix D information is significant because it would be useful to an attacker and it provides further evidence that the hackers were targeting PIPs. Nonetheless, Mr. Wagner's characterization seems to downplay the significance of the Appendix D.

Given the near certainty that PIPS and the information it held was a target before and confirmed during the 2014 incident response period, it is noteworthy that OPM's network monitoring technology did not have total visibility into PIPS. Wagner testified, "I guess it would be fair to say that there was minimum visibility of the PIPS application itself."[277] Despite this lack of visibility, OPM asserted they were confident no PII was taken during the course of the 2014 data breach. Wagner testified:

Q. Without monitoring tools on the PIP server at that point, at least insofar as this is described, could data from the PIPS application have been taken prior to March 28th and OPM had not been aware of that?

A. That would not be possible.

Q. Why is that?

[276] Saulsbury Tr. at 27-28.
[277] Wagner Tr. at 20.

A. Because it would have to pass through the distributing environment to do so. The mainframe sits within the center of the distributed nucleus, so in order to get data out, it would have to pass through all the other monitoring techniques.

Q. And why would that allow you to see it?

A. Because we had seen large sums of data leaving.

Q. And that would be –

A. -- we've seen large spikes and things of that nature, and DHS and us, both, looked for those large spikes at that time, and we did not see any.[278]

OPM has consistently asserted that no PII data was taken in the 2014 breach, but as US-CERT stated "additional documents may have been exfiltrated prior to March 2014, but there is no way to determine with exact certainty.[279] At a minimum sensitive data was in fact exfiltrated by the hackers, as evidenced by the items listed in Appendix D. The Appendix D data exfiltrated provided clues as the data targeted and the tactics, techniques and procedures (TTPs) of the attackers OPM monitored in 2014 provided hints about the data breach OPM later discovered in 2015.

Tactics Techniques & Procedures (TTPs) of Attackers Discovered in 2014: Hikit Malware and SMB Protocol

The attackers discovered in 2014 used Tactics, Techniques & Procedures (TTPs) —such as the type of malware and the attackers' ability to move throughout OPM's network—hinted at the targets of the attack OPM discovered in 2015. These TTPs also indicate the persistence, scope, and sophistication of attacks on OPM's network. Those key pieces of information, however, were not enough for OPM to stop the far more serious attack discovered in 2015. A public report by a threat analysis group has said the attackers discovered in 2014 used a specific and uncommon toolkit—or malware—designed for late-stage persistence and data exfiltration.[280]

The malware used by the attackers discovered in 2014 was identified as two variants of HiKit malware, referred to as HiKit A and HiKit B.[281] Notably, an October 2014 FBI Cyber Flash Alert said HiKit malware should be "given the highest priority for enhanced mitigation," and it "uses rootkit functionality to sit between the network interface card and the operating system enabling the malware to sniff all traffic to/from the compromised host."[282]

---

[278] Wagner Tr. at 20.
[279] June 2014 OPM Incident Report at HOGR0818 -001235.
[280] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 6.
[281] Saulsbury Tr. at 17; June 2014 OPM Incident Report Appendix C at HOGR0818-001244 - 1245.
[282] Cyber Div., Fed. Bureau of Investigation, A-000042-MW, *FBI Cyber Flash Alert* (Oct. 15, 2014), http://www.slideshare.net/ragebeast/infragard-hikitflash.

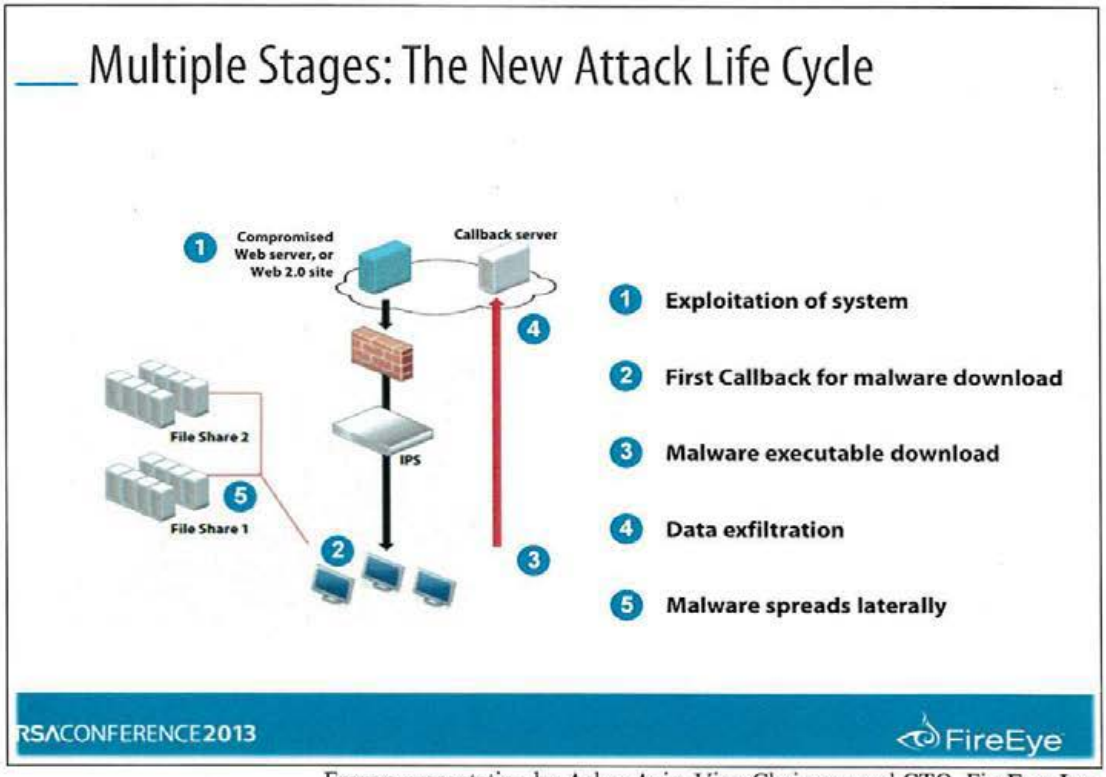
The use of HiKit malware is evidence of a sophisticated attacker that had achieved persistence on the IT environment, and was capable of performing a variety of functions (including data exfiltration) within OPM's network. In the 2014 Incident Report, US-CERT described Hikit as an "extremely stealthy form of malware designed to hide its malicious processes and programs from detection of commodity intrusion detection and anti-virus products."[283] Saulsbury described how the HiKit malware was used by the attackers discovered in 2014. He testified:

> So the fact that it is still beaconing means that an attacker could use it to still obtain entry into OPM's network. It just means that they could get onto that command and control server and start issuing commands to that infected machine. So C2 means command and control. As far as it being an IP rather a domain, that's not a significant issue. Basically, the way that their malware worked was there is a configuration file that tells the malware where to beacon out to. And instead of it having a domain that they created, they just put the IP directly in there, so instead of doing DNS resolution it just goes directly out, so it is just a quirk.[284]

Wagner described Hikit as a "form of a remote access tool, or RAC. It's a, basically, a back-door command tool," with "multiple functionalities. Most malware these days are kind of a Swiss Army knife type effect. You don't necessarily have a functionality like key logger. It usually utilizes multiple modules that allow various activities."[285] Wagner also said the Hikit malware was mostly used for persistence, or maintaining a presence at OPM, though keylogging activity was also observed.[286] Effectively, the malware was used so the hackers could "still use it to obtain entry into OPM's network."[287]

---

[283] June 2014 OPM Incident Report at HOGR0818 -001234.
[284] Saulsbury Tr. at 18-19.
[285] Wagner Tr. at 31.
[286] Wagner Tr. at 18.
[287] Saulsbury Tr. at 18.



From a presentation by Ashar Aziz, Vice-Chairman and CTO, FireEye, Inc. at RSA Conference USA 2013 (Feb. 28, 2013)

In other words, the Hikit malware is a rootkit—or a set of software tools that allow an unauthorized user to gain control of a computer system, escalate access, and persist in presence on the network without being detected. US-CERT explained that Hikit allowed the hackers to gain root level or administrator access to OPM's network and:

> [A]llow[ed] the attackers to create a reverse shell from their C2 [command and control] servers into the infected systems in OPM's network from a remote location anywhere in the world. The C2 servers are used to proxy the attackers' connections from their actual location on the Internet in order to keep their real identities and locations hidden. Hikit allows the attacker to run commands and perform functions from a remote location as if they had the equivalent of a monitor and keyboard connected to the compromised OPM system.[288]

The presence of Hikit on the OPM network was evidence of the adversary's presence and capabilities, but it did not reveal the initial point of entry. However, the use of a rootkit means the attackers had to have high level access to OPM's network. US-CERT said, the attacker was able to acquire high level credentials by exploit a vulnerability and likely obtained access to OPM's network using social engineering methods, such a phishing attack.[289] Outside threat analysis experts have described Hikit as a "late-stage persistence and data exfiltration tool" that

[288] June 2014 OPM Incident Report at HOGR0818 -001234.
[289] *Id.*

indicates the final phases of the threat actor's operational lifecycle.[290] The use of Hikit is evidence of a multistage operational lifecycle that would require the adversary to not only be well resourced, but also well organized.[291] The attack discovered in 2015 had similar characteristics.

The Hikit malware allowed the attackers to remain on OPM's systems—to maintain persistence—but in order to move throughout OPM's network undetected, the attackers used Server Message Block (SMB) protocols.[292] Hikit and SMB protocols are TTPs that tend to suggest "advanced penetration" and a sophisticated actor.[293]

With respect to the use of the SMB protocols, US-CERT said, "the malicious actors were connecting into the [redacted] server between the hours of 10pm and 10am EST with a compromised Windows domain administrator credential to search for PIPs related files on OPM's network file servers utilizing SMB commands."[294] Wagner described the attackers' use of SMB protocols during the 2014 attack. He testified:

> If you do some form of traversal or communications, you run over a normal communications protocol. It's not uncommon to change the protocol language or change the protocol ports in which you do traffic. And essentially, what they did is they tried to hide their activity and the things they were doing in a very highly utilized protocol port. So they basically hid their communications in the fuzz of the [network] traffic.[295]

Wagner acknowledged that the use of SMB protocols, in addition to other TTPs, were evidence of the threat actor's sophistication and capabilities. Wagner testified:

> Malware itself doesn't indicate sophistication. The other tactics and techniques that they utilized, or other things that they did, such as hiding their commands through, SMB, shows an advanced penetration. It's not a simple attack.[296]

The use of the Hikit malware and SMB protocols by the attackers discovered in 2014 show the attackers had a well-developed foothold in OPM's environment – and maintained a presence and persistence that indicated an advanced penetration that OPM was facing in 2014. NIST described the challenge of a persistent late stage penetration:

> [U]nderstanding threats and identifying modern attacks in their early stages is key to preventing subsequent compromises . . . preventing problems is often less costly and more effective than reacting to them after they occur. Thus, incident prevention is an important complement to an

---

[290] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 6.
[291] *Id.*
[292] June 2014 OPM Incident Report at HOGR0818 -001231.
[293] Wagner Tr. at 33.
[294] June 2014 OPM Incident Report at HOGR0818 -001233.
[295] Wagner Tr. at 16.
[296] Wagner Tr. at 31.

incident response capability. If security controls are insufficient, high volumes of incidents may occur.[297]

OPM's Network Logging Capabilities Limited Investigating the "How" and "How Long" for Attackers Discovered in 2014

OPM's ability to determine the "how" and "how long" of the attackers discovered in 2014 was limited by significant gaps in their capability to create, collect, and review audit logs of their network. Consequently, the answers to these questions remain unclear.

Audit logs are collections of events that take place on information technology systems and networks.[298] In the course of a forensic investigation, a variety of sources produce reviewable log information, including: antivirus software, firewalls, and intrusion detection and prevention systems.[299] These sources can help investigators piece together how the attacker gained access, where the attacker has been, how long they have been there, and, most importantly, give clues as to what the attackers are after.[300]

US-CERT identified numerous gaps in the centralized logging of security events at OPM during the investigation of the attackers discovered in 2014 stating: "Currently, OPM utilizes Arcsight as their SIEM [security information and event management] solution of choice, but there are numerous gaps in auditable events being forwarded to Arcsight for analysis, correlation, and retention."[301]

Gaps in OPM's audit logging capability likely limited OPM's ability to answer important forensic and threat assessment questions related to the incident discovered in 2014. This limited capability also undermined OPM's ability to timely detect the data breaches that were eventually announced in June and July 2015.[302] If IT security teams can track the attackers' movements back to the point of entry, they can patch the system vulnerabilities that allowed the penetration in the first place.

The OPM team did not, at the time of the incident discovered in 2014, have a robust logging capability that would have allowed them to determine the initial point of entry. Wagner acknowledged the audit logging gap and how that impacted their ability to identify the initial

---

[297] Paul Cichonski et. al., Nat'l Inst. of Standards & Tech., Spec. Pub. 800-61rev. 2, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* 2 (Aug. 2012), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[298] *See generally* Karen Kent & Murugiah Souppaya, Nat'l Inst. of Standards and Tech., Sp. Pub. 800-92, *Guide to Computer Security Log Management* (2006).

[299] *Id.*; *see also* Saulsbury Tr. at 15 (testifying that "There are many different log sources that we look at during a forensic investigation.").

[300] *E.g.* Wagner Tr. at 17-18; Saulsbury Tr. at 27.

[301] June 2014 OPM Incident Report at HOGR0818-001237.

[302] U.S. Office of Pers. Mgmt., Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015), https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/; U.S. Office of Pers. Mgmt., Press Release, *OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats* (July 9, 2015), https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.

point of entry. He stated: "I don't think we ever necessarily found initial point of presence or point of contact. Our last log entries at best, gave us the evidence of adversary presence, was November of 2013."[303] Wagner also testified:

> We did forensics to try to find the initial point of infection, but because we didn't have the full volume of logging that we have today throughout 2013 or 2012, or prior to the 2014 breach, we just ran into a point where there wasn't logs to give us sufficient evidence or indication of the exact point of presence.[304]

Saulsbury also acknowledged the limited logging capability. He stated:

> Q. Okay. And after all was said and done and you were looking back, when were the earliest actions taken by the hackers relating to the breach? And when did they take place? And what were they?
>
> A. So we don't know with 100 percent certainty what the initial entry point into the network was and when it was. So what we were able to do is look back through some of the logs that we had and try to find -- I can't remember at this point what the actual -- like our earliest log entry of activity was. I want to say that we had stuff, activity at least back in 2013 that was observed, but I can't recall at this point what the first evidence that we have is.[305]

The gaps in audit logs not only make it difficult to determine how the attackers perpetrated their hack of OPM, but also to determine with any degree of certainty how long the attackers were in the OPM network and any data exfiltrated. US-CERT said of the attackers discovered in 2014:

> It should be noted that the attackers had access to OPM's network since July 2012 and the documents below were exfiltrated during the time period of March 2014 and May 2014 when OPM CIRT started their advanced monitoring of the infected systems. Additional documents may have been exfiltrated prior to March 2014, **but there is no way to determine with exact certainty**.[306]

OPM also could not accurately assess the risks to their IT environment because the agency lacked the necessary logging information and centralization practices to generate a full picture of how the hackers established and then maintained persistence on OPM's systems. Threat and vulnerability information are the foundational step in implementing NIST's risk-based approach.[307]

---

[303] Wagner Tr. at 17-18.
[304] Wagner Tr. at 27.
[305] Saulsbury Tr. at 14-15.
[306] June 2014 OPM Incident Report at HOGR0818-001235.
[307] Comput. Sec. Div., Nat'l Inst. of Standards and Tech., *Risk Management Framework (RMF) Overview* (last updated Apr. 1, 2014), http://csrc.nist.gov/groups/SMA/fisma/framework.html.

The agency's inability to determine what other documents were exfiltrated prior to March 20, 2014 revealed two flaws in OPM's network monitoring practices. First, from March 2014 forward, US-CERT and OPM were installing the monitoring equipment, including additional logging capabilities, to determine what was being exfiltrated going forward. This left the agency with limited ability to look backwards. Second, the gaps in OPM's monitoring practices prevented OPM from determining what exactly was leaving the network and what data had been taken in the nearly two years the attackers had access to OPM's network.

After investigating the attackers discovered in 2014, US-CERT recommended OPM implement a robust system audit log data practice and:

> Require program offices to send critical system audit log data to Arcsight. During the system development life cycle, security related information and auditing requirements should be identified in accordance with OPM IT Security Policy and NIST recommended guidelines and configured to be sent to Arcsight for analysis, correlation, and retention. The following log sources were identified by Network Security as a high priority: Linux Secure Logs, HRTI Active Directory Logs, RACF authentication logs, and PIPS access logs. Aggregation of audit log data to centralized location such as Arcsight allows for proactive security monitoring and quicker time for triaging and remediating security incidents. (Low level of effort to implement).[308]

Wagner testified that OPM now (as of February 2016) has 100 percent visibility over their systems, but it is not clear when OPM gained this increased visibility. He stated:

> Q. Did you have total visibility over OPM's environment during the 2014 incident?
>
> A. I would not say 100 percent. We had a great deal of visibility. Actually, at the time, we had full visibility on the perimeter. Internal visibility, is where we had some gaps.
>
> Q. Why is that?
>
> A. As I said, it was an issue in which there was a longstanding project to have long entries loaded into the logger. Post the 2014 incident, that became a major priority, and we now have 100 percent visibility.[309]

It is notable that as Mr. Wagner admits they may have had significant visibility on the perimeter of the OPM network, but the gaps were more pronounced once the attacker was already inside the perimeter. Thus, an attacker already inside seemed to have the ability to move

[308] June 2014 OPM Incident Report at HOGR0818 -001237.
[309] Wagner Tr. at 33.

undetected across OPM's network. In a zero trust environment, an attacker's ability move once inside a network environment would be limited by a segmented environment and strong access controls.

As noted earlier, the attacker later discovered in 2015, had already established a foothold inside the OPM network as of early May 2014.

Chapter 3: OPM Attempts to Mitigate the Security Gaps Identified in 2014 While Iron Man and Captain America Go to Work (May 2014 – April 2015)

After the "Big Bang" effort on May 27, 2014, there were a number of events that inform the story of the data breaches announced in 2015. These events are also relevant to April 15, 2015—when OPM first identified an unknown SSL certificate[310] used to communicate with, an at the time, unknown domain: "opmsecurity.org."[311] "Opmsecurity.org" was later found to be registered to Steve Rogers—Captain America's alter ego. OPM subsequently identified another domain, "opmlearning.org," which was registered to Tony Stark—Iron Man's alter ego. These domains were part of an advanced and sophisticated attack infrastructure used to exfiltrate data from OPM in the summer of 2014.

As OPM and a multi-agency team began to investigate the scope and method of the attack, OPM enlisted the assistance of two contractors, Cylance and CyTech. The multi-agency team and contractors eventually made findings that caused OPM to announce in June and July 2015 that the personnel records for over 4 million individuals and background investigation data for over 20 million individuals had been compromised.[312]

To fully appreciate the May 2014 through April 2015 period, it is useful to establish OPM's posture with respect to mitigating the threat of the cyber incident that was identified in March 2014.

OPM's IT Security Posture and Mitigation Efforts After the May 2014 "Big Bang"

On June 22, 2014, US-CERT issued an Incident Report to OPM with fourteen observations and recommendations to address the security gaps identified in the aftermath of the 2014 cyber incident. The observations and recommendations in this Report highlighted the poor state of IT security at OPM and the failure to implement basic cyber hygiene practices.

The Incident Report directed OPM to "redesign their network architecture to incorporate security best practices."[313] Brendan Saulsbury, an OPM contractor who participated in OPM's 2014 and 2015 incident response efforts testified that US-CERT deemed OPM's network "**very insecure, insecurely architected" and found there was "lots of legacy infrastructure.**"[314]

---

[310] An SSL is a security sockets layer and is standard security technology used to establish an encrypted link between a server and a website.
[311] June 9, 2015 DMAR at HOGR0724-001154.
[312] U.S. Office of Pers. Mgmt., Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015), https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/; U.S. Office of Pers. Mgmt., Press Release, *OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats* (July 9, 2015), https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.
[313] June 2014 OPM Incident Report at HOGR0818-001235.
[314] Saulsbury Tr. at 16-17.

Saulsbury said this ultimately led to OPM's decision to "create basically a brand new hardened network" they called "the shell."[315] According to Saulsbury, OPM intended to eventually move legacy applications to the new shell.[316] US-CERT's 2014 Incident Report identified several specific technical recommendations to improve OPM's network security in the legacy environment, including buying security tools and reorganizing the OCIO.[317]

The US-CERT Incident Report included the level of effort required from OPM to implement each recommendation, from low to high. Three recommendations were considered "low" effort, four "moderate," and two "high."[318]

The US-CERT Incident Report found OPM did not have the capability to centrally manage and audit firewall access control lists and rules. Consequently, DHS recommended short and long term actions to combine manual auditing and scanning tools and then buy a network equipment solution to centrally manage configuration settings while also auditing these settings against best practices. This recommendation was considered "high level of effort."[319]

The Report also found OPM's network was "**extremely flat" and had "little to no segmentation**."[320] Thus, US-CERT recommended a redesign of network architecture with security best practices incorporated, including enforcing no direct user access to servers and requiring PIV credentials for access in order **to "limit an attacker's ability to move laterally across the network once initial access is obtained**."[321] This was a "high level of effort" recommendation.

The recommendations that required a low level of effort to implement were related to logging, security awareness training, and a redesign of OPM's Incident Response Plan.

In recommendations related to the OCIO, US-CERT found "**there is a gap in information technology leadership across OPM as an agency**" and that "**it is not uncommon for existing policies to be circumvented in order to achieve business functions while exposing the entire agency to unnecessary risk.**"[322] In response, US-CERT recommended OPM undertake a policy review and gap analysis to determine the need for additional policies to manage IT security and business functions and noted a "cultural change will need to occur to ensure policies are never circumvented unless absolutely required."[323] DHS also recommended

---

[315] Saulsbury Tr. at 16-17.
[316] *Id.*
[317] June 2014 OPM Incident Report at HOGR0818-001235. *See also* OPM Cybersecurity Events Timeline. The OPM Cybersecurity Events Timeline states that the OPM Security Operations Center (SOC) began unofficially reporting to the OPM CIO in April 2014, and officially began reporting to the OPM CIO in March 2015 after the union approved the reorganization. As of March 22, 2015, the relevant unions at OPM formally approved the OCIO reorganization.
[318] June 2014 OPM Incident Report at HOGR0818-001236 -39.
[319] June 2014 OPM Incident Report at HOGR0818-001236.
[320] *Id.*
[321] *Id.*
[322] June 2014 OPM Incident Report at HOGR0818-001238.
[323] *Id.*

reorganizing the OCIO.[324] Among other things, the reorganization shifted the Director of Security Operations to report to the CIO.[325]

Documents and testimony show OPM began to implement the DHS recommendations in or around May or early June of 2014. The effort continued through early 2016. Based on testimony from two witnesses involved in responding to the 2014 incident, it appears OPM tried to implement DHS's recommendations, but the agency was hindered by the fact that it started with a woefully unsecure network. Throughout this phase, the attackers involved in the data breaches announced in 2015 had already established a foothold on the OPM network.[326]

Key 2014 US-CERT Recommendations Highlighted OPM IT Security Vulnerabilities

One of DHS's key recommendations was to ensure all OPM users were required to use PIV cards for access to the OPM network.[327] In a 2015 OMB Report on IT security, OPM was identified at the end of fiscal year 2014 as one of several agencies with the "weakest authentication profile[s]"—meaning a majority of the agency's unprivileged users logged on only with a user ID and password, making an unauthorized access more likely.[328] The OMB Report also stated that at OPM, only one percent of user accounts required PIV cards for access.[329] Wagner, Director of IT Security Operations stated PIV card enforcement did not fully roll out until September 2014, and was being implemented through early 2015.[330] He added the FIS [Federal Investigative Services] contractors (who did the background investigations) were the last group required to have PIV cards for access.[331]

Had OPM leaders fully implemented the PIV card requirement – or two-factor authentication – security controls when they first learned hackers were targeting background investigation data, they could have significantly delayed or mitigated the data breach discovered in 2015. The agency first learned attackers were targeting background investigation data on

---

[324] June 2014 OPM Incident Report at HOGR0818-001238.
[325] OPM Cybersecurity Events Timeline.
[326] Wagner Tr. at 75-78 (discussing implementation status of two recommendations); Saulsbury Tr. at 31-34 (discussing implementation status of six recommendations and noting logging capability gaps remain due to technical difficulties applying the logging function to mainframes); June 9, 2015 DMAR at HOGR0724-001154.
[327] In August 2004, the federal government initiated several initiatives to enhance cybersecurity across the federal government, including Homeland Security Presidential Directive 12 (HSPD-12). HSPD-12 established a mandatory government-wide standard for secure and reliable identification for access to government IT systems and facilities that was further defined as a requirement for personal identity verification (PIV) credentials. Then OMB directed federal agencies to issue and use PIV cards to control access. OMB reported that as of the end of fiscal year 2014, only 41 percent of all agency user accounts at the CFO Act agencies required PIV cards to access agency IT systems.
Cyber Threats and Data Breaches Illustrate Need for Stronger Controls Across Federal Agencies: Hearing Before Subcomm. on Research & Tech. and Subcomm. on Oversight of the H. Comm. on Science, Space & Tech., 114th Cong. (July 8, 2015) (testimony Gregory C. Wilshusen, Dir. of Info. Sec. Issues Gov't Accountability Office).
[328] Office of Mgmt. & Budget, Exec. Office of the President, *FY 2014 Annual Report to Congress: Federal Information Security Management Act* at 23 (Feb. 27, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.
[329] *Id.* at 20.
[330] Wagner Tr. at 38, 75.
[331] Wagner Tr. at 75.

March 20, 2014.[332] Yet the first data major exfiltration — involving 21.5 million individuals' background investigation files — did not occur until early July 2014, giving the agency over three months to implement security controls to protect those data.[333] Testimony from the Department of Homeland Security revealed that OPM's implementation of two-factor authentication for remote logons in January, 2015 — which was already required of federal agencies — "stopped the adversary from taking further significant action."[334] If OPM leadership had implemented two factor authentication even earlier, for example in April or May of 2014, the agency might have locked out attackers before they had a chance to commit the most significant digital violation of national security faced to date.

In July 2015, OMB launched a "cybersprint" to require all agencies to expedite implementation of cybersecurity measures, including enforcement of PIV card access, within 30 days. According to OPM, 100 percent of their privileged users were required to use PIV cards as of April 2015, but only 41 percent of their unprivileged users were required to use PIV cards. The agency improved its PIV card compliance—by July, 97 percent of unprivileged users were required to use PIV cards.[335]

In August 2015, OPM updated its PIV card implementation status in response a request from the Committee. The agency reported "approximately 99 percent of OPM users are required to use a PIV card (or equivalent) to access OPM workstations with two-factor authentication."[336] The agency also told the Committee that OPM bought 5,000 ActivClient licenses in 2009 to enable the use of PIV card credentials to access OPM workstations and further clarified that currently 8,400 such licenses "are activated, current, and operational."[337] The agency's response raised questions as to the status of the 5,000 licenses purchased in 2009 and why PIV card enforcement was not a priority earlier, particularly given that OMB had identified OPM as an agency with one of the "weakest authentication profile[s]."[338] The use of basic cyber hygiene practices, such as full implementation and enforcement of PIV card access, would have limited the damage incurred during the 2015 data breach incidents.

---

[332] Dep't of Homeland Security/US-CERT and OPM, OPM Cybersecurity Events Timeline (Aug. 26, 2015) (OPM Production: May 13, 2016).
[333] *Id.*
[334] *Under Attack: Federal Cybersecurity and the OPM Data Breach: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2015) (statement of Andy Ozment, Assistant Secretary for Cybersecurity & Communications, Department of Homeland Security) (adversary activity June 2014 to January 2015, stopped by security control rolled out January 2015); *see* Dep't of Homeland Security/US-CERT and OPM, OPM Cybersecurity Events Timeline (Aug. 26, 2015) (OPM Production: May 13, 2016) (security control rolled out January 2015 was two factor authentication for remote access).
[335] Office of Mgmt. & Budget, Exec. Office of the President, *CyberSprint Results* (July 31, 2015) (On file with the Committee).
[336] Letter from Jason Levine, Dir. Congressional, Legislative & Intergovernmental Affairs, U.S. Office of Pers. Mgmt., to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Aug. 28, 2015).
[337] *Id.*
[338] Office of Mgmt. & Budget, Exec. Office of the President, *FY 2014Annual Report to Congress: Federal Information Security Management Act* 23 (Feb. 27, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf..

OPM Efforts to Buy Security Tools to Secure the Legacy Network and Rebuild OPM's "Very Insecure, Insecurely Architected Network"

In response to US-CERT observations and recommendations in the 2014 Incident Report, OPM launched a multi-phase IT Infrastructure improvement project to (1) buy security tools to secure their legacy network and (2) create an entirely new network environment.

Former OPM CIO Donna Seymour testified to the Committee this project began after the March 2014 cyber incident.[339] In May 2014, Seymour contacted Imperatis, an IT security contractor, to discuss the project. In an email to former colleagues at Imperatis, Seymour wrote: "[D]o you recall all the work we did at MARAD [U.S. Maritime Administration] to straighten out a very messy network with poor security? Well . . . I'm looking for an expert consultant who can guide me and my team through the exact same thing."[340] Seymour and two Imperatis employees worked together at MARAD.[341]

Ultimately, these discussions led to a sole source contract award to Imperatis for the multi-phased IT Improvement project, in June 2014.[342] The project included four phases:

(1) Tactical (securing the legacy IT environment).

(2) Shell (creating a new data center and IT architecture).

(3) Migration (migrating all legacy IT to the new architecture).

(4) Cleanup (decommissioning legacy hardware and systems).

Phase 1, or the Tactical phase, supported OPM's effort to buy security tools to secure the agency's legacy IT environment immediately following the 2014 incident. The Tactical phase of the project began in June 2014 and was completed in September 2015.[343]

OPM's efforts to buy security tools involved interactions with a number of contractors, including Cylance and CyTech which would later provide cybersecurity and forensic solutions to

---

[339] *OPM Data Breach: Hearing Before the H. Comm. On Oversight and Gov't Reform*, 114th Cong. (June 16, 2015) (testimony of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).

[340] Email from Donna Seymour, Chief Info Officer, U.S. Office of Pers. Mgmt., to Patrick Mulvaney and [redacted] Imperatis (May 10, 2014, 9:46 a.m.), Attach. 12 at 001463 (Imperatis Production: Sept. 1, 2015).

[341] *Id.*; Imperatis Proposal Volume II – Staffing and Management, Attach. 5a at 262-264, 268-270 (Appx. A: Key Personnel Resumes), (Imperatis Production: Sept. 1, 2015).

[342] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000003 (Imperatis Production: Sept. 1, 2015). The OPM OIG raised concerns about the sole source nature of this contract but did acknowledge given the urgency need to secure the OPM legacy network making a sole source award for purposes of buying security tools (Tactical phase) was reasonable. U.S. Office of Pers. Mgmt., Report No. 41-CI-00-15-055, *Flash Audit Alert – U.S. Office of Personnel Management Infrastructure Improvement* Project 5 (June 17, 2015) [hereinafter OIG Flash Audit Alert (June 17, 2015)].

[343] Letter from Imperatis to H. Comm. on Oversight & Gov't Reform Majority Staff (Feb. 12, 2016) (on file with the Committee).

OPM.[344] Documents and testimony show Cylance began conversations with OPM about their products through a reseller, and CyTech was introduced to OPM through Imperatis.

The Committee obtained documents that show OPM was buying and deploying at least ten security tools to the legacy IT environment. Websense is one such tool. In 2014, Websense had limited functionality and simply filtered users' web traffic to prevent access to certain sites (like gambling sites).[345] The agency had to upgrade Websense because, according to Saulsbury, the old version "wasn't performing" and did not include the "advanced capabilities" such as web filtering, email and data security functionality.[346] Saulsbury also testified that in 2014, the Websense server was not the primary target.[347] Saulsbury believed the Personnel Investigations Processing System (PIPs) was the target.[348]

The Websense upgrade was identified as a Priority 1 task and OPM quickly made a purchase in June 2014, but the phased deployment of this tool was not completed until September 2015.[349] As of February 2015, there were continuing challenges with the Websense pilot and as of April 2015 the project status for Websense was only at about 60 percent complete.[350] Saulsbury testified one of the deployment challenges was balancing "usability and security," but, after the 2014 incident, there was less resistance from users and security became the higher priority.[351] In April 2015, according to OPM, the first indicators of compromise were detected (including the unknown SSL certificate that was beaconing to the domain "opmsecurity.org") during the roll out of the upgraded version of Websense.[352]

The agency purchased another tool to improve network access control: [redacted][353] The agency purchased [redacted] on July 28, 2014, and deployed it from September 2014 - September 2015.[354] Documents show the [redacted] deployment was delayed at least in part by required notifications to relevant unions. In August 2015, an Imperatis Weekly Report stated that "project sponsor [for [redacted]] is in notification stage with the Union" and the proposed mitigation strategy to "prepare updated project timeline, plan & memo to pilot [redacted] to non-Union Agency users.[355]

In the aftermath of the 2014 incident, OPM attempted to implement DHS's recommendations, including buying new security tools and building a new IT environment, but

---

[344] *See Infra* Chapters 4, The Role of Cylance and Chapter 5, The CyTech Story.
[345] Saulsbury Tr. at 17-18.
[346] Saulsbury Tr. at 49.
[347] Saulsbury Tr. at 17-18.
[348] *Id.*
[349] OPM Tactical Toolset: Purchase, Kick-off and Completion Timeframes (Oct. 21, 2015) (Imperatis Production: Oct. 21, 2015); Saulsbury Tr. at 50.
[350] Imperatis Weekly Report (Apr. 13, 2015-Apr. 17, 2015), Attach. 6 at 000737 (Imperatis Production: Sept. 1, 2015); Imperatis Weekly Report (Apr. 20, 2015-Apr. 24, 2015), Attach. 6 at 000753 (Imperatis Production: Sept. 1, 2015).
[351] Saulsbury Tr. at 53.
[352] Saulsbury Tr. at 58-59.
[353] Imperatis Monthly Program Review (July-Aug. 2014), Attach. 7 at 000973 (Imperatis Production: Sept. 1, 2015).
[354] OPM Tactical Toolset: Purchase, Kick-off and Completion Timeframes (Oct. 21, 2015) (Imperatis Production: Oct. 21, 2015).
[355] Imperatis Weekly Report (Aug. 3, 2015-Aug. 7, 2015), Attach. 6 at 000942 (Imperatis Production: Sept. 1, 2015).

because of the state of IT security at OPM was so poor, there was much to do. The agency, however, missed opportunities to prioritize the purchase and deployment of certain cutting edge tools that, as Cylance CEO Stuart McClure testified, "would have prevented this attack."[356] Meanwhile, as OPM worked to deploy badly needed security tools, Captain America and Iron Man were exfiltrating sensitive data from OPM's unsecure IT environment in the summer of 2014.

OPM Missed Key Developments

The Committee obtained evidence that shows OPM was working to respond to the attackers discovered in the spring through the summer of 2014, while the attacker groups who ultimately stole background investigation and personnel records data were moving through the agency's network. OPM did not discover the attackers responsible for the background investigation data breach – until April 2015 when it was too late. These attackers had already established a foothold in OPM's network as of early May 2014 and began to exfiltrate this data in early July 2014. Meanwhile, OPM continued its mitigation efforts in response to the attackers discovered in 2014. Documents and testimony show a timeline of key events that provide context for data breach discoveries made beginning in April 2015:

- **July 2012** – Attackers had access to OPM's network.[357]
- **November 2013** – The first known adversarial activity begins in OPM's network that led to the breach identified by US-CERT in March 2014.[358]
- **December 2013 –** Adversarial activity to harvest credentials from OPM contractors begins by the attackers later identified in April 2015.
- **March 20, 2014** – US-CERT notified OPM of malicious activity and OPM initiates investigation and monitoring of adversary.
- **March 2014 to May 2014 –** OPM (under US-CERT guidance) investigated 2014 incident and monitored attackers.
- **April 25, 2014** – The domain "Opmsecurity.org" is registered to Steve Rogers (a.k.a. Captain America).[359] This domain was later used to exfiltrate data from OPM's network.
- **May 7, 2014** – The attacker poses as a background investigations contractor employee (KeyPoint), used an OPM credential, remotely accessed OPM's network and installed PlugX malware to create a backdoor. The agency's forensic logs show "infected machines" were accessed through a VPN connection, which was how background

[356] McClure Tr. at 18.
[357] June 9, 2015 DMAR at HOGR0724-001154.
[358] *Hearing on OPM Data Breach: Part II* (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).
[359] Saulsbury Tr., Ex. 4.

investigation contractors accessed OPM's network. At the time, OPM gave contractors a username and password and investigators would log in with this OPM credential.[360]

- **May 27, 2014** – OPM initiates "Big Bang" to eliminate attackers and complete remediation. This decision was made after OPM observed the attackers "load a key logger onto . . . several database administrators' workstations" and they got "too close to getting access to the PIPs system."[361] Meanwhile, the attacker that established a foothold on May 7, 2014 remained in the OPM network.

- **June 5, 2014 –** Malware is installed.[362] This malware installation appears to have been facilitated through the backdoor established on May 7, 2014.[363]

- **June 2014** – OPM contractor USIS self-detects a cyber-attack on its IT system and notified OPM.[364] USIS investigates and blocks and contains the attacker by early July, and invites US-CERT to USIS facilities to investigate by late July 2014.[365]

- **June 20, 2014** – Attackers conduct a remote desktop protocol (RDP) session indicating the attackers had escalated their access and began moving deeper into the network, contacting "important and sensitive servers supporting . . . background investigation processes." This RDP session was not discovered until 2015.[366]

- **June 23, 2014** – First known adversary access to OPM's mainframe, according to US-CERT.[367]

- **July to August 2014** – Attackers successfully exfiltrate OPM background investigation data. OPM contractor Brendan Saulsbury testified that forensic logs showed "they are sort of touching or accessing the data during the summer of 2014."[368]

---

[360] Wagner Tr. at 127-128; Saulsbury Tr. at 70-71; OPM Cybersecurity Events Timeline; Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016). KeyPoint CEO testified that "there was an individual who had an OPM account that happened to be a KeyPoint employee and [] the credentials of that individual were compromised to gain access to OPM." *Hearing on OPM Data Breach: Part II* (statement of Eric Hess, KeyPoint CEO). The OPM Director of IT Security Operations [Wagner] said multiple credentials were compromised during the 2015 incident, but a KeyPoint credential was likely used for the initial attack vector. [Wagner] added "the adversary, utilizing a hosting server in California, created their own FIS investigator laptop virtually. They built a virtual machine on the hosting server that mimicked and looked like a FIS investigator's laptop…and they utilized a compromise KeyPoint user credential to enter the network through the FIS contractor VPN portal." Wagner Tr. at 86.

[361] Saulsbury Tr. at 25-26, at 25-26.

[362] Letter from KeyPoint Government Solutions to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (July 2, 2015).

[363] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016).

[364] *Hearing on OPM Data Breach: Part II* (statement of Robert Giannetta, Chief Info. Officer, U.S. Investigations Serv's, LLC). Despite a contractual obligation to notify contractors immediately of a "new or unanticipated threat or hazard", OPM did not notify their contractors (KeyPoint and USIS) of the March 2014 incident. *Id.*

[365] *Hearing on OPM Data Breach: Part II* (statement of Robert Giannetta, Chief Info. Officer, U.S. Investigations Serv's, LLC).

[366] Coulter Tr., Ex. 18.

[367] OPM Cybersecurity Events Timeline.

- **July 29, 2014** – The domain "Opm-learning.org" is registered to Tony Stark (a.k.a. Iron Man).[369]

- **August 2014** – Following public reports of a data security breach at another contractor, OPM requested access to KeyPoint facilities and KeyPoint agreed.[370]

- **August 16, 2014** – The malware installed on June 5, 2014 appears to cease operational capabilities.[371]

- **October 2014** – Attackers move through the OPM environment to the Department of Interior data center where OPM personnel records are stored.[372]

- **December 2014** – Attackers exfiltrate 4.2 million personnel records.[373]

- **March 3, 2015 -** "wdc-news-post[.]com" is registered by attackers. Attackers would use this domain for C2 and data exfiltration in the final stage of the intrusion.[374]

- **March 9, 2015** – Last beaconing activity to the unknown domain "opmsecurity.org" registered to Captain America, attackers switched their attack infrastructure to "wdc-"news-post.com" as their primary C2 domain for the remainder of the intrusion. [375]

- **April to June 2015** – Primary incident response and investigation period.

The timeline outlined above sets the stage for the incident response and forensic investigation that took place in the spring of 2015.

In April 2015, OPM Realized They Were Under Attack – Again

On April 15, 2015, OPM sent an email to US-CERT reporting the presence of four malicious binaries, and what would later turn out to be the first indicators that OPM's systems had been compromised in the largest data breach in the history of the federal government.[376]

---

[368] Saulsbury Tr. at 70. Wagner, the OPM Director of IT Security Operations admitted OPM did not have a "fully logged" environment in the summer of 2014, but they were working toward that end during the summer and through the fall of 2014. Wagner Tr. at 78.
[369] Saulsbury Tr., Ex. 4.
[370] *Hearing on OPM Data Breach: Part II* (statement of Eric Hess, Chief Exec. Officer, KeyPoint Gov't Solutions).
[371] Letter from KeyPoint Government Solutions to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (July 2, 2015) (citing US-CERT Report (Aug. 30, 2015).
[372] OPM Cybersecurity Events Timeline.
[373] *Id.*
[374] DOMAIN > WDC-NEWS-POST.COM, THREATCROWD.ORG (last visited June 28, 2016), https://www.threatcrowd.org/domain.php?domain=wdc-news-post.com..
[375] Saulsbury Tr. at 59; *see also* DOMAIN > WDC-NEWS-POST.COM, THREATCROWD.ORG, available at: https://www.threatcrowd.org/domain.php?domain=wdc-news-post.com.
[376] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-465355 (May 4, 2015) (OPM Production: Oct. 28, 2016); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).

Documents and testimony show the initial discovery of the indicators of compromise (IOCs) involved a number of parties, including US-CERT, the FBI, OPM contractors, the OPM IG, and several private companies.

Captain America: The First Indicator that Led to the 2015 Discovery of the Background Investigation Data Breach

In April 2015, OPM discovered and began investigating the first indicator that its systems had been compromised.[377] Director of IT Security Operations Jeff Wagner testified that the first indicator of compromise was an unknown SSL certificate,[378] and was discovered during the rollout of a new version of the security application "Websense."[379] A Secure Socket Layer (SSL) certificate is used to establish a secure channel between an individual's browser and a website. In this case, an OPM computer had been communicating with an unknown website, or domain: "opmsecurity.org."

The Committee obtained documents that show the unknown domain opmsecurity.org was initially brought to the attention of OPM by a contractor, Assurance Data, during the roll out of a new functionality for OPM's Websense technology.[380] Assurance Data identified opmsecurity.org in an email with the subject "RE: OPM Daily Health" on April 14, 2015.[381] OPM was adding groups of users to Websense, as they were transitioning towards filtering all outbound traffic through Websense.[382] During the course of this rollout, Assurance Data observed "a certificate error for the domain called opmsecurity.org."[383]

The next day, April 15, OPM responded to Data Assurance. In an email, an OPM employee described the domain opmsecurity.org as "sketchy at best."[384] The agency "looked up the domain details and observed that it was what appeared to be a spoof domain,"[385] or a domain that was purposely named to emulate legitimate looking websites belonging to or affiliated with OPM. There were clues that "opmsecurity.org" was a spoof domain: "it was a randomized email address,"[386] and it was registered to Steve Rogers, a.k.a. Captain America.

OPM provided to the Committee a document entitled "AAR Timeline" that provided more information about their findings on April 15 and 16 related to the unknown SSL certificate.

---

[377] June 9, 2015 DMAR at HOGR0724-001154; *see also* Saulsbury Tr. at 57-58.
[378] Wagner Tr. at 80.
[379] Saulsbury Tr. at 58.
[380] *Id.*
[381] Email from [redacted] Chief Sec. & Strategy Officer, Assurance Data, Inc. to [redacted] [redacted] et. al., U.S. Office of Pers. Mgmt. (Apr. 14, 2015, 12:36 p.m..) at HOGR020316- 1887 (OPM Production: Apr. 29, 2016).
[382] Saulsbury Tr. at 58.
[383] *Id.*
[384] Email from [redacted] U.S. Office of Pers. Mgmt. to [redacted] Chief Sec. & Strategy Officer, Assurance Data, Inc., and [redacted] et al, U.S. Office of Pers. Mgmt. (Apr. 15, 2015, 9:50 a.m.) at HOGR020316- 1886 (OPM Production: Apr. 29, 2016).
[385] Saulsbury Tr. at 59.
[386] ThreatConnect Research Team, *OPM Breach Analysis*, THREATCONNECT (June 5, 2015), available at: https://www.threatconnect.com/opm-breach-analysis/..

According to this document, the unknown SSL certificate "[W]as identified and attached to domain "opmsecurity.org" and "six machines [were] identified as communicating with this domain."[387] The AAR Timeline also reported that the domain "opmsecurirty.org" was registered to "a fake email address" under the name "Steve Rogers."[388] Further, the AAR Timeline, noted that an "alert" related to this unknown SSL certificate was initially discovered on February 24, 2015 and the original beaconing traffic to this domain began in December 2014.[389] The AAR Timeline also indicated OPM had identified three work stations and three servers on the OPM network that communicated with the suspicious domain "opmsecurity.org."[390]

The investigation revealed that these machines had also contacted another potentially malicious domain "opm-learning[.]org" – which was registered to Tony Stark, a.k.a. Iron Man – and "wdc-news-post.com." Two of the three suspicious IP addresses—each registered to a Marvel comic book character—was "a really big red flag" for OPM's security team.[391] After running forensic scans OPM was able to determine the suspicious IP address registered to Tony Stark ("opm-learning[.]org") was in fact communicating with malware that was trying to "fly under the radar as if it was a McAfee antivirus executable."[392] This was noteworthy because OPM did not use McAfee.[393] Beginning in 2005, US-CERT had issued alerts that APT attacks often used malware specifically designed to elude anti-virus software and firewalls and mentioned the use of McAfee and Symantec names in connection with these attacks.[394]

After identifying the false IP addresses and the malware, OPM alerted US-CERT.[395] At 6:53 p.m. on April 15, 2015, OPM's Computer Incident Readiness Team (OPM-CIRT) filed a report, INC478069, identifying four malicious binaries – files that OPM considered to potentially be malware or other malicious code. Three of the four malicious binaries reported to US-CERT on April 15, 2015 were identified as having the "potential for a breach or a compromise passed a malware infection."[396] Wagner, OPM's Director of IT Security Operations, also contacted the FBI's CYWATCH to report that the IP addresses and domains associated with the incident as potential C2 servers—the infrastructure necessary for an adversary to conduct an attack.[397]

The Avengers: Anatomy of the Data Breach Discovered in 2015

The first evidence of the attackers' presence comes on May 7, 2014, when the attackers dropped malware (PlugX) onto an OPM server that was one hop away from a machine with

---

[387] AAR Timeline – Unknown SSL Certificate (April 15, 2015) at HOGR020316- 1922 (OPM Production: Apr. 29, 2016).
[388] *Id.*
[389] *Id.*
[390] Saulsbury Tr. at 59.
[391] Saulsbury Tr. at 60.
[392] *Id.*
[393] *Id.*
[394] US-CERT, *Technical Cyber Security Alert TA05-189A: Targeted Trojan Email Attacks* (July 2005)
[395] Saulsbury Tr. at 60.
[396] Coulter Tr. at 14-15.
[397] Email from REDACTED, Fed. Buerau of Investigation Cyber Div to Jeff Wagner, Dir. Info. Tech. Security Operations, U.S. Office of Pers. Mgmt. (Apr. 16, 2015, 2:19 a.m.) at HOGR020316- 1910 (OPM Production: Apr. 29, 2016); *see also* AAR Timeline – Unknown SSL Certificate (April 15, 2015) at HOGR020316- 1922 (OPM Production: Apr. 29, 2016).

direct access to the background investigations and finger print database.[398] Ultimately, these attackers were able to access OPM's Local Area Network (LAN)—the foundational component of OPM's internet infrastructure—and drop PlugX malware.[399]

The PlugX malware, which is a sophisticated piece of malware, allowed the attackers to maintain a presence on OPM's system and network as of May 7, 2015, and it also provided the attackers with other functionality. This malware has an estimated 19,000 lines of code and comes with 13 default, modular plugins.[400] It provides an attacker with a "range of functionality" including the ability to log keystrokes; modify and copy files; capture screenshots or video of user activity; and perform administrative tasks such as terminating processes, logging off users, and rebooting victim machines.[401] PlugX has the ability to give attackers "complete control over the [infected] system."[402]

The PlugX malware, which was the primary piece of malware used in the 2015 data breach, was engineered to covertly beacon back to the "host's network resources [and] establishing a SSL connection to malicious domains (opmsecurity[.]org and wdc-news-post[.]com) and setting the state of a TCP connection."[403] In effect, an SSL connection establishes a secure, or encrypted, link between a server and a website – which in this case was established between the PlugX malware and the malicious domains ("opmsecurity.org" and "wdc-new-post.com").

US-CERT also found these attackers used "opmsecurity.org", primarily associated with the IP address [redacted], as part of their attack infrastructure—the internet components necessary for the attackers to communicate with their PlugX malware throughout the life-cycle of the intrusion.[404] Further, US-CERT found (based on domain firewall logs) that the compromised machines on OPM's network connected with "known malicious IP [redacted]" on January 12 and January 20, 2015.[405]

Other variations of PlugX were found to have been active within the OPM environment throughout the 2014/2015 intrusion. The attacker placed additional, modified versions of PlugX—dubbed by investigators as the "first" and "second" variations—on victim machines on October 10, 2014 and January 31, 2015, respectively.[406] These versions of PlugX were installed months after the key objectives of the intrusion were already achieved. This shows the attacker was continuously modifying and customizing PlugX in order to better customize the malware to OPM's network environment, maintain access, and conceal malicious activities.

---

[398] June 9, 2015 DMAR at HOGR0724-001154.
[399] OPM Cybersecurity Events Timeline.
[400] Roman Vasilenko & Kyle Creyts, *An Analysis of PlugX Malware*, LASTLINE LABS (Dec. 17, 2013), http://labs.lastline.com/an-analysis-of-plugx.
[401] Ryan Angelo Certeza, Pulling the Plug on PlugX, TRENDMICRO (Oct. 4, 2012), http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/112/pulling-the-plug-on-plugx.
[402] *Id.*
[403] June 9, 2015 DMAR at HOGR0724–001154.
[404] June 9, 2015 DMAR at HOGR0724-001167.
[405] *Id.*
[406] June 9, 2015 DMAR at HOGR0724–001154.

On a related matter, the security research firm ThreatConnect published a February 2015 analysis of the Anthem breach announced on February 4, 2015 that mentioned the "opm-learning.org" domain.[407] Anthem is a health insurance company that held data on as many as 80 million Americans—current and former members of Anthem health plans, and some nonmembers.[408] ThreatConnect attributed the Anthem hack to a threat actor group, variously described as "Deep Panda."[409] In February 2015 (over one month before OPM's April 2015 discovery), ThreatConnect found that this group may have also registered the domain opm-learning.org as part of an intrusion campaign, and noted "OPM had been compromised by a likely state-sponsored Chinese actor in mid-March of [2014]."[410] ThreatConnect warned that because the domain was registered after the breach occurred on July 29, 2014, "OPM could be an ongoing direct target of Chinese state-sponsored cyber espionage activity."[411]

In March 2015, it appears that the attackers changed their attack infrastructure. The attackers switched their command and control servers, installing a new, updated version of malware on infected systems.[412] Consequently, on March 7, 2015, the attackers registered the domain wdc-news-post.com, resolving to the IP address [redacted][413] The domain would switch IP's to [redacted] on May 11, 2015, after the intrusion was already discovered.[414] The switch from opmsecurity.org ([redacted]) to wdc-news-post.com ([redacted]) was accompanied by a new version of PlugX malware, dubbed the "third version" by US-CERT, which would be programed to call-back to the newly-created "wdc-news-post.com" domain.[415]

The March 2015 change in the attack infrastructure could have been prompted by a number of factors. First, it is not uncommon for attackers to use different infrastructure during different stages of the intrusion life-cycle. It is possible large-scale data exfiltration had been completed by spring 2015 and the attackers were moving to a new infrastructure wholly unconnected from that used to effect the initial entry into OPM's network. In the event this intrusion and theft of data was discovered, the infrastructure used would be compromised.

Second, changing the infrastructure would allow the attackers to maintain access to the network should their previous infrastructure be discovered. It is possible open-source threat researchers were dangerously close to independently discovering infrastructure used in the OPM intrusion.

---

[407] Threatconnect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.
[408] Michael Hiltzik, *Anthem is Warning Consumers About its Huge Data Breach. Here's a Translation*, L.A. TIMES, Mar. 6, 2015, http://www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html.
[409] Threatconnect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/
[410] *Id.*
[411] *Id.*
[412] June 9, 2015 DMAR at HOGR0724-001157.
[413] DOMAIN > WDC-NEWS-POST.COM, THREATCROWD.ORG (last visited June 28, 2016), https://www.threatcrowd.org/domain.php?domain=wdc-news-post.com.
[414] June 9, 2015 DMAR at HOGR0724-001157.
[415] *Id.*

The version of PlugX used in the 2014/2015 intrusion had a suite of capabilities that were likley customized for the OPM environment. In describing the malware, US-CERT delineated the capabilities of the particular version of PlugX used in the 2014/2015 intrusion:[416]

> [T]his version of PlugX also is capable of remote access control, file/directory/drive enumeration, file/directory creation, process creation, enumerating the host's network resources, establishing a SSL connection to malicious domains (opmsecurity[.]org and wdc-news-post[.]com) and setting the state of a TCP connection.[417]

The ability to establish an "SSL connection to malicious domains" would become a critical component in the hacker's ability to execute command and control, maintain access, and exfiltrate data out of OPM's network. Hackers used the PlugX to create fake SSL certificates that would allow host machines to connect to the malicious domains "opmsecurity.org", "opm-learning.org", and "wdc-news-post.com."[418] The use of these SSL certificates eventually led to the discovery of the intrusion. In April 2015, OPM security personnel began installing Websense, which gave OPM an enhanced ability to filter SSL certificates.[419] During the Websense roll-out, the newly installed system was able to flag fake SSL certificates to "opmsecurity.org" and other malicious domains.

It is not entirely known how, or even when, the attackers gained access to an OPM network credential held by OPM's contractor KeyPoint, but the attackers were able to use that credential to gain initial access into OPM's network, using a virtual private network (VPN) login to access an OPM SQL server. The attackers also setup remote desktop protocol (RDP) sessions from the SQL server to move laterally, infected additional systems and gained additional footholds until finally connecting to their primary target, the background investigation and fingerprint databases.

The KeyPoint credential was "utilized for the initial vector of infection,"[420] but a number of compromised credentials were used over the course of the data breach.[421] The credential that was used at the initial vector of infection, the point at which the adversary dropped malware to obtain persistent presence, was being used by a KeyPoint employee's account.[422] But that KeyPoint employee did not have administrator credentials, which are necessary to conduct higher-order functions on IT environment. Jeff Wagner testified:

> So the adversary utilized tactics in order to gain domain administrator credentials. Exactly **how they obtained the credentials, we don't have forensic evidence for, but they needed to gain another set of credentials to do operations**. It's not the only set of credentials they utilized to perform operations. So there are multiple stages where various

[416] June 9, 2015 DMAR at HOGR0724 – 001154.
[417] June 9, 2015 DMAR at HOGR0724 – 001154.
[418] Saulsbury Tr. at 58-59.
[419] Saulsbury Tr. at 58-59.
[420] Wagner Tr. at 86.
[421] Wagner Tr. at 86.
[422] Wagner Tr. at 86.

> credentials were used, and though us enforcing PIV killed the capability of them utilizing the KeyPoint credential, they still had persistence from the malware. So they were able to get into the environment through another method to maintain persistence and then utilize domain.[423]

After gaining access to the SQL server, the attacker opened a RDP and dropped malware to maintain a presence on the SQL server. The SQL server itself is significant for its use as the "back end storage" for various OPM applications, including a Jumpbox server used by the administrators that had access to background investigation data. Saulsbury testified "this jumpbox had access into the environments, into the network segments that contained the background investigation systems."[424] The attackers used an RDP to enter the jumpbox and use it "as a pivot point to access all of the systems that were firewalled off from [the] normal network."[425]

The move from the SQL server to the jumpbox was a "lateral movement" by the hackers, and it demonstrates their ability to maintain a presence on OPM's systems, and also to gain the necessary administrator credentials necessary to move from system to system, from computer to computer. Using the jumpbox as a "pivot point," the attackers were able to access the PIPS mainframe, which stored the background investigation data, and "all the FTS boxes" which "are related to the fingerprint transmission system," and finally the human resources department's systems with personnel records stored on systems hosted by the Department of the Interior.[426]

These lateral movements, as evidenced by RDP sessions and the timestamps on the PlugX variants, continued from May into June of 2014.[427] With access to OPM's mainframe as early as June 23, 2014 (and less than one month after the May 27, 2014 "Big Bang"), the attacker would have had access to mainframe applications such as the background investigation data stored on the PIPS system.[428] By early July 2014, the attackers began to exfiltrate the background investigation data. Evidence of data exfiltration would appear to OPM and US-CERT in the form of encrypted RAR archives—"stashes" of stolen data.[429] The attackers continued to exfiltrate the background investigation data through August of 2014,[430] but the fingerprint transaction system data was not taken until March 26, 2015.[431]

---

[423] Wagner Tr. at 86.
[424] Saulsbury Tr. at 75
[425] *Id.*
[426] Saulsbury Tr. at 76-77.
[427] Coulter Tr., Ex. 18.
[428] OPM Cybersecurity Events Timeline.
[429] Coulter Tr. at 25-26. Mr. Coulter would go on to describe the attackers' use of RAR files to exfiltrate data saying, "so as is common in a lot of APT cases, or actually a lot of breaches, if their end goal is to collect data, then they're going to search for it and bring it back to a central point for aggregation. A lot of times data, like this email, if you were to compress it, it would be, you know, potentially one-100th of the size. So RAR, which is a compression format, is used to shrink data. You can also then apply a password to it. So in a lot of cases, where there is data exfiltration or a confirmed breach, it's very common to find these compressed, encrypted stashes of whatever bad guys were after." *See also* June 9, 2015 DMAR at HOGR0724-001156.
[430] OPM Cybersecurity Events Timeline.
[431] June 9, 2015 DMAR at HOGR0724-001158.

The time period from early July 2014, when the attackers begin to exfiltrate the background investigation data, to April 24, 2015, when OPM "successfully eliminates [the] adversary from their systems" represents the data breach end-stage.[432] In this final phase, where the attacker achieves their primary objective – whether it is accessing and exfiltrating data or some other malicious activity – it is important to note this end-stage would have been preceded by an initial penetration through OPM's defenses, an intelligence gathering phase to learn about OPM's network, systems, and security measures. Then after all of this activity the attacker would finally drop the malware and set up the domains necessary to collect and extract data.

The details of the initial phases of the attack and how the 2015 attackers penetrated OPM's defenses and gained sufficient knowledge of OPM's systems so as to quickly begin exfiltrating data, likely will never be known. What is known is how OPM discovered the data breaches announced in June and July of 2015 and how OPM, their interagency partners, government contractors, and private sector incident responders took OPM from the initial indicators of compromise discovered on April 15, 2015 to remediation of the incident in June 2015. Between the first sign of the attackers' foothold on May 7, 2014,[433] to the first exfiltration of data in early July 2014,[434] OPM would complete the "Big Bang"[435] to expel from their network the attackers discovered in 2014. From OPM's perspective by the end of May 2014, the 2014 incident was over – little did OPM know that the 2015 data breach operation was underway.

The following chapter provides additional details on OPM's 2015 discovery and incident response efforts that ultimately led to the discovery of background investigation and personnel records that were exfiltrated – from the perspective of an OPM contractor called Cylance, which was brought in to assist OPM in April 2015.

---

[432] OPM Cybersecurity Events Timeline.
[433] OPM Cybersecurity Events Timeline.
[434] OPM Cybersecurity Events Timeline.
[435] Email from Press Secretary, U.S. Office of Pers. Mgmt., to Jeff Wagner, Dir. of IT Sec. Operations, U.S. Office of Pers. Mgmt. (June 18, 2015, 8:01 p.m.) at HOGR 020316-000266-67 (OPM Production: Feb. 16, 2016).